

II 39.452
BCU IASI - ECONOMIE



Elena GRECU
Raluca COMĂNESCU
Georgiana TRIFAN

GDPR
pentru afaceri

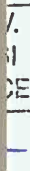
**Un ghid
eficient**
pentru

companii

Recomand, cu multă încredere și deosebită plăcere, lecturarea și studierea cărții „GDPR pentru afaceri”, elaborată de experții firmei Grecu & Asociații, pe care îi cunosc și cu care colaborez de peste 2 ani, desfășurând împreună activități profesionale în domeniul GDPR și de formare/instruire în cadrul mai multor firme și al Facultății de Informatică a Universității Titu Maiorescu.

Este o carte pe limbajul antreprenorilor, ușor de citit și de aplicat în orice societate.

Conf. univ. dr. ing. **IUSTIN PRIESCU**
Decan al Facultății de Informatică, UTM.ro



71 39452

Elena Grecu

Raluca Comănescu

Georgiana Trifan

GDPR PENTRU AFACERI. UN GHID EFICIENT PENTRU COMPANII

GDPR PENTRU AFACERI.
UN GHID EFICIENT PENTRU
COMPANII

UNIVERSITATEA
"B. P. HASDEU" IASI

Universitat Juridică
București
2021

BCU IASI / CENTRAL UNIVERSITY LIBRARY

Elena Grecu

Raluca Comănescu

Georgiana Trifan

R17 6

15849

GDPR PENTRU AFACERI. UN GHID EFICIENT PENTRU COMPANII



0 000008 69270

BCUIASI

Universul Juridic

București

-2021-

Editat de Universul Juridic SRL.

Editura Universul Juridic este acreditată CNATDCU (lista A2) și este considerată editură cu prestigiu recunoscut.

Copyright © 2021, Universul Juridic SRL.

Toate drepturile asupra prezentei ediții aparțin Universul Juridic SRL.

Nicio parte din această lucrare nu poate fi copiată fără acordul scris al Universul Juridic SRL.

! Niciun exemplar din prezentul tiraj nu va fi comercializat fără ștampila și semnătura Editurii sau, după caz, a Autorului/Autorilor, aplicate pe interiorul ultimei coperte.

Respect pentru autorii noștri, respect pentru profesia aleasă!

Prezenta lucrare, în tot sau în parte, este purtătoare de drepturi de autor, aflate sub protecția Legii nr. 8/1996 privind dreptul de autor și drepturile conexe. Întrucât, în contemporaneitate, aceste drepturi sunt ignorate și încălcate într-o măsură alarmantă, în pofida sistemului valorilor și convențiilor sociale nescrise, a devenit necesară apărarea lor prin forța și sub sancțiunea legii.

UNIVERSUL JURIDIC SRL, titular al dreptului de autor asupra prezentei lucrări, precizează pentru cititorii săi:

- 🔪 conform art. 196 din Legea nr. 8/1996, constituie infracțiune și se pedepsește cu închisoare de la o lună la un an sau cu amendă reproducerea, fără autorizarea sau consimțământul titularului drepturilor recunoscute de lege, a operelor purtătoare de drepturi de autor sau a produselor purtătoare de drepturi conexe;
- 🔪 conform art. 14 din Legea nr. 8/1996, prin reproducere se înțelege realizarea, integrală sau parțială, a uneia ori a mai multor copii ale unei opere, direct sau indirect, temporar ori permanent, prin orice mijloc și sub orice formă, inclusiv realizarea oricărei înregistrări sonore sau audiovizuale a unei opere, precum și stocarea permanentă ori temporară a acestora cu mijloace electronice.

Editura își rezervă dreptul de a acționa, prin mijloace legale și prin implicarea autorităților competente, în vederea protejării drepturilor patrimoniale de autor al căror deținător este în baza contractelor de editare.

Descrierea CIP a Bibliotecii Naționale a României

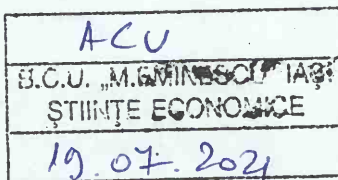
GRECU, ELENA

GDPR pentru afaceri : un ghid eficient pentru companii / Elena Grecu, Raluca Comănescu, Georgiana Trifan. - București : Universul Juridic, 2021
ISBN 978-606-39-0704-3

I. Comănescu, Raluca

II. Trifan, Georgiana

34



Redacție:
tel.: 0732.320.666
e-mail: redactie@universuljuridic.ro

Distribuție:
tel.: 021.314.93.15
fax: 021.314.93.16
e-mail: distributie@universuljuridic.ro
editurauniversuljuridic.ro



Editura Universul Juridic



Portal:
tel.: 0725.683.560
e-mail: portal@universuljuridic.ro
universuljuridic.ro



Universul Juridic



Librăria UJmag:
tel.: 0733.673.555; 021.312.22.21
e-mail: comenzi@ujmag.ro
ujmag.ro



UJmag.ro

Cuprins

GDPR-UL DIN PUNCTUL DE VEDERE AL AFACERILOR (COMPANIILOR/SOCIETĂȚILOR) – IMPACTUL ECONOMIC ȘI ORGANIZAȚIONAL.....	13
BUNE PRACTICI ÎN MANAGEMENTUL ȘI ADMINISTRAREA COMPANIEI.....	28
Implementarea clauzelor GDPR în actul constitutiv al firmei și în AGA.....	28
Adunarea Generală a Asociațiilor.....	31
Implicarea administratorului în luarea măsurilor tehnice și organizatorice și în monitorizarea lor. Numirea unui DPO/DPC	32
Monitorizarea măsurilor tehnice și organizatorice	35
Cooperarea între administrația societății și DPO/DPC.....	36
GDPR și controalele de la autoritățile publice. Registrul unic de control	38
Registrul unic de control	40
Asigurarea implementării GDPR la punctele de acces în societate.	
Recepția și poarta	41
Procedura de acces în companie	41
Supravegherea video	44
Verificarea identității prin sisteme tehnice și imagini.....	48
Alte date prelucrate la punctele de acces	52
Puncte de recepție multi-task	53
Stabilirea fluxului de date cu caracter personal în societate	54
Registrul de prelucrare	58
Modificări legislative și impactul în activitatea de prelucrare.....	60
Arhivarea sau distrugerea documentelor care conțin date cu caracter personal	62
Principii generale	62
Elementele principale înregistrate de companii.....	63
Suportul de arhivare	65
Persoanele desemnate.....	66
BUNE PRACTICI ÎN DEPARTAMENTELE JURIDIC, FINANCIAR ȘI DE RESURSE UMANE	68
Aplicarea GDPR în departamentul juridic. Bune practici.....	69
Scopurile prelucrării.....	69

Temeiurile de prelucrare la nivelul departamentului juridic	70
Responsabilitățile personalului din departament.....	71
Procedura de soluționare a cererilor și a plângerilor.....	73
Procedura soluționării plângerilor împotriva răspunsului la o cerere.....	76
Registrul GDPR pentru contracte	78
Proceduri recomandate pentru conformarea cu GDPR a departamentului financiar/contabil. Bune practici.....	81
Fluxul operațional al prelucrării datelor cu caracter personal.....	82
Procedură pentru decontarea sumelor pentru concediile medicale.....	82
Întocmirea documentelor pentru încasări și plăți. Facturarea	84
Procedura de prelucrare a datelor cu caracter personal în cadrul gestionării procesului de recuperare a creanțelor	86
Tipurile de date colectate în departamentul financiar-contabil. Particularități și exemple.....	88
Date prelucrate de departamentul financiar contabil.....	88
Înmânarea fluturașilor de salariu	88
Acordarea tichetelor de masă.....	89
Decontarea cheltuielilor pentru deplasări	90
Proceduri recomandate pentru conformarea cu GDPR a departamentului de HR. Bune practici.....	92
Tipuri de activități desfășurate de departamentul resurse umane.....	93
Tipuri de date cu caracter personal prelucrate de departamentul de resurse umane.....	93
Prelucrarea de date în faza de recrutare. Particularități.....	94
Despre prelucrarea datelor din cazierul judiciar	95
Legitimațiile de serviciu, pontajele și permisele de parcare	97
Prelucrarea datelor cu caracter personal privind confesiunea religioasă.....	101
Prelucrarea imaginilor salariaților prin foto/video	102
Monitorizarea video a angajaților care utilizează mijloace de transport în comun puse la dispoziție de angajator.....	102
Camerele supraveghere amplasate în incinta de lucru a angajaților	103
Publicarea fotografiilor și videoclipurilor de la activitățile individuale sau colective profesionale și extra-profesionale.....	104
Administrarea dosarelor de personal. Tipuri de date prelucrate. Bune practici.....	107
Eliberarea adeverințelor care atestă corectitudinea datelor. Scrisori de recomandare.....	109

Prelucrarea datelor în timpul unei cercetări disciplinare.....	111
Mijloacele de comunicare utilizare cu și de către salariați	112
BUNE PRACTICI ÎN DEPARTAMENTELE DE MARKETING, VÂNZĂRI ȘI CLIENT SUPPORT	114
Departamentul de Marketing	114
Descrierea activităților de marketing la nivel intern	116
Scopurile prelucrării datelor cu caracter personal în departamentul de marketing.....	117
Legalitatea prelucrării datelor cu caracter personal (temeiuri legale) de către departamentul de marketing	118
Prelucrarea se bazează pe consimțământul persoanei vizate.....	119
Condițiile pe care trebuie să le îndeplinească consimțământul	120
Pentru ce perioadă se acordă consimțământul?	124
Retragerea consimțământului.....	125
Consimțământul copiilor	127
Bune practici privind obținerea consimțământului	129
Prelucrarea se bazează pe un interes legitim	132
Activități specifice Departamentului de Marketing în contextul GDPR	134
Site-ul societății. Bune Practici	134
Politica de confidențialitate	137
Cookie-uri. Politica de cookies a site-ului companiei	139
Profilarea, un instrument de marketing din ce în ce mai des folosit de către companii.....	142
Organizarea de concursuri și campanii promoționale	146
Promovarea produselor pe rețelele de socializare	148
Abonarea la newsletter	148
Publicarea articolelor de presă	149
Bune practici privind aplicarea GDPR-ului în domeniul Marketing	150
Departamentul de Vânzări.....	151
Datele cu caracter personal prelucrate care se prelucrează de către Departamentul de Vânzări.....	152
Temeiurile prelucrării datelor cu caracter personal	153
Bune practici ale Departamentului de Vânzări în domeniul datelor cu caracter personal	154
Departamentul de Client Support	155
Datele cu caracter personal prelucrate care se prelucrează de către Departamentul de Client Support	156
Temeiul prelucrării datelor cu caracter personal	156

Bune practici ale Departamentului de Client Support în domeniul datelor cu caracter personal	156
Informarea persoanelor vizate asupra drepturilor pe care acestea le au	157
MĂSURI TEHNICE ȘI ORGANIZATORICE	161
Responsabilitatea operatorului. Privacy by design & by default.....	161
Măsuri tehnice	166
Securizarea echipamentelor prin intermediul cărora se prelucrează date cu caracter personal	168
Autentificarea unică a membrilor personalului.....	168
Executarea copiilor de siguranță	170
Anticiparea incidentelor de securitate ce ar putea rezulta din pierderea sau furtul unui echipament	170
Securizarea serverelor.....	171
Protejarea rețelei interne de internet	172
ISO27 001:2013.....	172
Măsuri organizatorice	173
Planul de conformare.....	173
DPO-ul	175
Evidența activităților de prelucrare	177
Analiza interesului legitim	185
Instruirea salariaților	186
Limitarea accesului	191
Politici și proceduri.....	192
Politica privind exercitarea drepturilor persoanelor vizate.....	195
Dreptul de acces la date	195
Dreptul la rectificare	197
Dreptul de a fi uitat.....	197
Dreptul la restricționarea prelucrării.....	198
Dreptul la portabilitate.....	199
Dreptul la opoziție	200
Dreptul de a nu face obiectul unei decizii automate	200
Dreptul la retragerea consimțământului.....	201
Dreptul de a formula o plângere la autoritatea de supraveghere	201
Dreptul de a se adresa instanțelor de judecată	203
Politica privind retenția datelor	203
Procedura pentru incidente de securitate	206
Evaluarea partenerilor comerciali	209
Notele de informare	209

Informarea salariaților și a aplicanților pentru un post disponibil în cadrul companiei	210
Informarea partenerilor clienților	211
Informarea vizitatorilor	211
Consultarea reprezentanților angajaților cu privire la sisteme ce presupun prelucrări de date în spațiile în care se desfășoară activitate.....	212
Acordurile privind protecția datelor cu caracter personal	214
Auditul intern	217
Auditul preliminar	217
Raportul de audit	218
PRACTICA AUTORITĂȚILOR.....	220
Clasamentul sancțiunilor prin raportare la încălcări	222
Clasamentul sancțiunilor prin raportare la cuantumul amenzilor	222
Clasamentul sancțiunilor prin raportare la numărul amenzilor	223
Analiza măsurilor dispuse de autoritățile de supraveghere.....	223
Austria.....	223
Belgia.....	226
Bulgaria.....	231
Croația	237
Cipru	238
Cehia	240
Danemarca	243
Estonia.....	245
Finlanda	246
Franța	247
Germania	249
Grecia	259
Italia	263
Letonia	269
Lituania	270
Malta	270
Olanda	271
Polonia.....	273
Portugalia.....	276
România	277
Slovacia	287
Spania.....	289
Suedia.....	294

Ungaria	297
Modalitatea prin intermediul căreia este inițiată o investigație	309
Controlul efectuat de ANSPDCP este întotdeauna anunțat?	311
Pot amâna efectuarea unei investigații anunțate?	312
Desfășurarea efectivă a procedurii investigației	313
Efectuarea investigațiilor pe teren	314
Efectuarea investigațiilor la sediul ANSPDCP	316
Efectuarea investigațiilor în scris	316
Aspecte particulare privind investigațiile desfășurate la autoritățile/organismele publice	318
Procesul-verbal încheiat de ANSPDCP. Elemente componente.	
Căi de atac. Posibile sancțiuni.....	319

Prefață

Înainte de prefața cărții vreau să vorbesc despre „a scrie în ziua de azi”. Cine mai are nevoie de informații din cărți în epoca platformelor și vitezei, cine mai are timp să citească atunci când ar putea să ia concluziile gândite de alții deja și, pe scurt, oare ce le motivează pe tinerele autoare să scrie?

Nu e mai ușor să plătești publicitate sau să vorbești la o emisiune TV?

Cred că a scrie este o obligație a oricărui intelectual care lucrează cu concepte – atunci când scrii nu ai doar dreptul de exprimare, dar și obligația de a fi consistent. Atunci când scrii și recitești ești și arhitect, și constructor, dar și consumator de idei, altfel nu poți depăși o pagină sau două. Într-o epocă a volumului și vorbitului, este nevoie de mai multă responsabilitate și, înainte de toate, este nevoie să vedem scrisul ca pe o lucrare personală, ca o parte din moștenirea pe care o minte scripitoare trebuie să se asigure că o transmite și altora, că o împarte cu cititorii.

Trecând mai departe, tema cărții este provocatoare – dreptul ca disciplină este un dinozaur viu, pentru că legile sunt pentru și despre oameni și societăți. Cu fiecare carte scrisă despre legi și despre modul cum funcționăm se clădește o conștiință colectivă a ceea ce înseamnă societate, reguli, ce este acceptabil, despre bine și rău. Pe lângă interes, cartea de față este o lucrare folositoare și întărește nu doar obligația de a scrie, dar și obligația de a interpreta și provoca principiile vechi la noile realități.

Sunt legi și principii vechi de mii de ani, care încă stau la baza relațiilor noastre, și există și legi noi pentru provocări noi – cum este GDPR, consecința avântului globalizării și tehnologizării din viața fiecărui om.

Interesant pentru mine este că citatul din începutul cărții pune legislația GDPR sub semnul vechii bătălii din Lumea Nouă și Bătrânul Continent, aducând demnitatea în centrul societății, ca o valoare esențială a ființei umane. Sunt idei umaniste cărora în sfârșit le-a venit vremea. Eliberat de foame și sclavie sub diferite forme, omul de rând își caută sensul și limitele libertății.

Libertatea de a înțelege ce se întâmplă cu informațiile despre tine, libertatea de a-ți administra opțiunile personale, precum și multe altele detaliate în prezenta carte sunt de fapt o digitalizare a relațiilor omenești în care ideile sunt noile valori și cursa este despre a înțelege opțiunea

maselor. Deciziile în timp real impun reguli în timp real care să reechilibreze balanța de putere între algoritmi și oameni. Legile referitoare la protecția datelor vin să așeze lucrurile în societate și tocmai de aceea acest subiect este nu doar actual, dar mai ales relevant în viitor. Tehnologia și inteligența artificială avansează exponențial. E timpul ca oamenii să înțeleagă cine folosește informațiile, cum arată noua media, de ce personalizarea vine cu prețul viziunii și pentru cine implementăm de fapt GDPR.

Este o mare bucurie și onoare să fiu o mică parte din această lucrare care încearcă să ne aducă mai aproape legile și regulile – care ni se aplică, indiferent dacă le înțelegem sau nu. De fapt, cartea este un exercițiu de (auto)educație și tocmai de aceea vă felicit că o aveți în brațe și vă urez lectură plăcută!

Monica CADOGAN
CEO și fondator Vivre

GDPR-UL DIN PUNCTUL DE VEDERE AL AFACERILOR (COMPANIILOR/SOCIETĂȚILOR) – IMPACTUL ECONOMIC ȘI ORGANIZAȚIONAL

„A fi european înseamnă a avea dreptul ca datele tale cu caracter personal să fie protejate de legi puternice, europene. Pentru că europenilor nu le plac dronele care zboară pe deasupra lor și le înregistrează fiecare mișcare, nici companiile care contabilizează fiecare click pe mouse.

De aceea, Parlamentul, Consiliul și Comisia au convenit în mai anul acesta un regulament comun privind protecția datelor cu caracter personal. Acest regulament este o lege europeană fermă aplicabilă companiilor, indiferent de locul în care își au sediul și ori de câte ori prelucrează datele dumneavoastră cu caracter personal. Pentru că, în Europa, păstrarea confidențialității datelor personale contează. Această chestiune ține de demnitatea umană”.

Jean Claude Juncker

Tuturor ne place să măsurăm – fie că vorbim despre profit, cifra de afaceri, marjă sau alți indicatori – ne place să raportăm și să ne raportăm la cifre. În cazul apariției GDPR-ului cei mai mulți s-au raportat la cât business s-a pierdut din cauza apariției Regulamentului European, câți bani s-au cheltuit pe consultanți, cât timp s-a pierdut pentru a răspunde la chestionare și câțiva s-au raportat la ce amenzi au avut de plătit.

Mai puțini s-au gândit la ce a însemnat pentru organizația lor implementarea unor reguli pentru a respecta GDPR-ul, schimbarea organizării uneori chiar și a culturii organizaționale.

Foarte puțini oameni de afaceri s-au gândit la partea bună a lucrurilor, la securitatea sporită a datelor și a businessului implicit care a venit o dată cu implementarea GDPR-ului.

Noi, autoarele, ne propunem să explicăm pe înțelesul neprofesioniștilor ce trebuie să întreprindă o societate pentru a se conforma prevederilor GDPR. Astfel, fie că sunteți juristul din cadrul unei societăți, fie că lucrați în departamentul de Marketing sau Resurse Umane, fie că sunteți chiar administratorul societății, ne dorim ca această carte să fie un punct de sprijin pentru călătoria de conformare. Deși se spune că se poate

preciza cu exactitate momentul începerii implementării, dar niciodată nu se va ști când se va finaliza, GDPR-ul fiind un domeniu în care trebuie menținută atenția și concentrarea pe toată durata de viață a societății, ne propunem ca limbajul să fie unul accesibil (să ieșim din zona de „pășarească” a specialiștilor), astfel încât să putem sprijini cât mai multe persoane dornice să înțeleagă GDPR-ul. Cartea nu se dorește a fi una exhaustivă, dedicată specialiștilor, ci este una practică, cu multe exemple din experiența noastră, a autoarelor – care practică avocatura de afaceri, concentrându-se inclusiv pe protecția datelor, de mai bine de 17 ani.

După cum se știe, datele au valoare pecuniară. Având valoare financiară, ele se comercializează pe piață. Fac obiectul intermediarilor și al unui comerț intens. Analytics, big data, market profiling, inteligența artificială (AI), blockchain, IoT (internet-of-things) etc. – sunt doar câteva domenii notorii și prezente pe piața digitală.

Toate domeniile economiei și finanțelor în activitatea curentă, gestionează baze masive de date (banking, asigurări, servicii medicale private, contabilitate etc.) și își construiesc strategiile pe baza unor intense și din ce în ce mai sofisticate operațiuni de profilare și prelucrare a datelor personale.

Datelor personale le este recunoscută valoarea comercială în mod explicit inclusiv prin Directiva privind Contractele de furnizare de conținut digital și de servicii digitale din 26 martie 2019 (ce va trebui transpusă în legislația națională până la 01.07.2021), recunoscându-se datelor personale valoare de piață, prin care se achită un serviciu: *„Prezenta directivă se aplică și atunci când comerciantul furnizează sau se angajează să furnizeze consumatorului conținut digital sau un serviciu digital, iar consumatorul furnizează sau se angajează să furnizeze comerciantului date cu caracter personal (...)”*. Monetizarea, inclusiv pe cale legislativă a valorii datelor personale, este o realitate juridică.

Dar nu doar societățile din domeniul tehnologiei folosesc baze de date – datele cu caracter personal ale clienților sunt folosite de clinici, grădinițe și școli, magazine online, agenții de turism și recrutare etc., dar toate societățile dețin date cu caracter personal ale angajaților.

Deși se discută atât de mult de General Data Protection Regulation – (Regulamentul General privind Protecția Datelor), se pare că doar o parte din companiile europene au implementat obligațiile GDPR (cifrele diferă în funcție de sursă – mai puțin de jumătate, conform IAPP (International Association of Privacy Professionals) sau două companii din trei, conform unui studiu realizat de RSM pentru European Business Awards¹.

¹ <https://www.rsm.global/news/30-european-businesses-are-still-not-compliant-gdpr>.

De asemenea, se discută foarte mult de cât costă implementarea normelor GDPR – conform International Association of Privacy Professionals (IAPP), cele mai bogate 500 firme au cheltuit 7.8 miliarde de dolari pe implementarea GDPR, bugetul mediu pentru fiecare firmă fiind de 16.000.000 \$. Pe de altă parte, autoritățile naționale (inclusiv Comisia Europeană) insistă pe faptul că nu ar trebui cheltuite sume foarte mari, ci doar respectate normele impuse de GDPR, pornind de la principiile enumerate în preambulul regulamentului.

Este evident că investiția în soluțiile de securitate pentru criptarea datelor, asigurarea confidențialității, detectarea posibilelor amenințări, gestionarea răspunsurilor către persoanele vizate și mai ales pregătirea permanentă a angajaților presupune costuri, existând soluții scumpe și soluții ieftine, procese acoperitoare și dosare cumpărate „de-a gata” fără a fi implementate.

În ciuda costurilor, majoritatea companiilor au considerat că implementarea GDPR nu a dăunat dezvoltării lor – 65% dintre respondenți au considerat că GDPR a avut un impact pozitiv asupra afacerii lor și doar 15% au considerat că GDPR a avut un impact negativ asupra activității lor.²

La împlinirea unui an de la aplicarea GDPR, Comisia Europeană a publicat un raport conform căruia 67% dintre europeni au auzit de GDPR, în timp ce 57% dintre aceștia știu de existența unei autorități publice în fiecare țară care se ocupă de protejarea drepturilor lor în ceea ce privește datele cu caracter personal și către care pot trimite plângeri pentru încălcarea acestor drepturi.³

Chiar și în momentul pandemiei – o perioadă dificilă pentru toate statele lumii, în Europa nu s-a oprit discuția despre GDPR și despre importanța datelor cu caracter personal – fie că vorbim despre date de sănătate (temperatură), fie că vorbim despre numele persoanelor infectate sau despre localizarea lor exactă. De asemenea, societățile au trebuit să își completeze politicile privind prelucrarea datelor cu caracter personal pentru cazurile în care angajații aveau anumite boli cronice care ar fi presupus o precauție suplimentară.

Ce este GDPR?

GDPR reprezintă Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor

² GDPR Compliance Status TrustArc https://info.trustarc.com/Web-Resource-2018-07-12-GDPR-ResearchReport_TYP.html.

³ https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf.

fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).⁴ GDPR a fost publicat în Jurnalul Oficial al Uniunii Europene L119/4 mai 2016, a intrat în vigoare la 25 mai 2016 și este aplicabil din 25 mai 2018 la nivelul întregii Uniuni Europene.

GDPR nu reprezintă o noutate absolută, fiind de fapt doar o adaptare a Directivei 95/46/CE la modificările tehnologice și cerințele sporite privind securitatea datelor cu caracter personal.

Se vorbește de schimbări extraordinare, unii numesc o revoluție în domeniul protecției datelor – noi vrem doar să punctăm noutățile din domeniul protecției datelor cu caracter personal, subliniind faptul că GDPR:

- sporește drepturile individuale ale persoanelor vizate de colectarea și prelucrarea datelor cu caracter personal;
- lărgeste spectrul categoriilor de date cu caracter personal;
- impune noi obligații operatorilor de date cu caracter personal, precum și persoanelor împuternicite de aceștia, obligații care cu un impact tehnic și organizațional;
- stabilește amenzi semnificative în caz de neconformitate;
- impune în unele cazuri numirea unui DPO (Data Protection Officer – Responsabil de date cu caracter personal), persoană care trebuie să se asigure de aplicarea coerentă a dispozițiilor legale pentru a da eficiență acestora față de persoanele vizate.

Regulamentul este inclus în categoria documentelor care formează Cadrul european în domeniul securității cibernetice alături de alte trei documente (Convenția privind criminalitatea informatică, Directiva privind măsurile pentru un nivel comun ridicat de securitate a rețelilor și a sistemelor informatice și Strategia de securitate cibernetică a Uniunii Europene).

Acest regulament a influențat și alte legislații naționale, fiind un model pentru Brazilia, Japonia, China, Rusia și California. În Statele Unite, California a fost primul stat cu o mai bună protecție a datelor pentru cetățenii săi. În ceea ce privește forma și conținutul, acest Act de confidențialitate a consumatorilor din California (CCPA)⁵ este în mod clar comparabil cu GDPR european. De asemenea, în aprilie 2016, Republica Turcia a publicat Legea privind protecția datelor cu caracter personal w.

„Data protection by design” și „data protection by default”.

⁴ <http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679>.

⁵ The California Consumer Privacy Act (CCPA) a intrat în vigoare pe 01.01.2020.

nr. 6698, în Monitorul Oficial. La cererea reprezentanților afacerilor turce, termenul pentru această înregistrare a fost amânat pentru 30.06.2020 când autoritatea turcă va putea începe amendarea celor care nu s-au conformat.

Cerut cu insistență de asociațiile de consumatori, scopul a fost acela de a proteja persoanele fizice, mai ales în contextul în care marile corporații au folosit și o parte din ele încă folosesc datele personale în moduri greu de înțeles pentru persoanele obișnuite, precum și pentru a determina companiile să acorde o atenție mai mare protecției datelor.

„Unul dintre principalele scopuri ale Regulamentului general privind protecția datelor este de a da mai multă putere oamenilor și de a le oferi mai mult control asupra uneia dintre cele mai valoroase resurse din economia modernă – datele lor. Putem atinge acest obiectiv numai dacă și când oamenii devin pe deplin conștienți de drepturile lor și de consecințele deciziilor lor.

Începem deja să vedem efectele pozitive ale noilor reguli. Cetățenii au devenit mai conștienți de importanța protecției datelor și a drepturilor lor. Și acum își exercită aceste drepturi, așa cum realizează autoritățile naționale de protecție a datelor în activitatea lor de zi cu zi. Au primit până acum peste 95.000 de reclamații din partea cetățenilor.” (Declarație comună a Vice-Președintelui Timmermans, Vice-Președintelui Ansip, Comisarului European Jourová and Gabriel, cu ocazia Zilei Internaționale a Datelor cu caracter personal, 25.01.2019)

Ce sunt datele cu caracter personal?

„Datele cu caracter personal” au fost definite în cadrul Regulamentului ca fiind „orice informații privind o persoană fizică identificată sau identificabilă („persoană vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;”

Foarte important de reținut este faptul că datele personale nu se limitează la elemente ușor de înțeles precum CNP-ul, adresă, nume, adresa de email etc., ci aria este mult mai extinsă în noul regulament, cuprinzând și informații legate de localizarea prin GPS, adrese IP, asigurări, date părinți și copii, date biometrice, datele referitoare la preferințele de cumpărare, religie, sex, etnie sau locul de muncă.

Exemple de date care nu sunt considerate a fi date cu caracter personal:

- CUI-ul/CIF-ul unei societăți;
- O adresă de e-mail care are formatul info@numecompanie.com, secretariat@numecompanie.ro, vanzari@numecompanie.eu;
- Sediul unei societăți;
- Datele anonimizate;
- Numărul de telefon al unei societăți publicat pe pagina sa web.

Normele GDPR se aplică numai datelor cu caracter personal privind persoanele fizice și nu reglementează datele referitoare la societăți sau la alte entități juridice.



Atenție! Cu toate acestea, informațiile legate de societăți alcătuite dintr-o singură persoană pot constitui date cu caracter personal dacă permit identificarea unei persoane fizice (numele societății este Vasile Ion SRL cu sediul la domiciliul domnului Vasile Ion, număr de telefon: numărul de telefon al domnului Vasile Ion).



Atenție! Normele se aplică, de asemenea, tuturor datelor cu caracter personal referitoare la persoane fizice în cadrul unei activități profesionale, cum ar fi angajații unei societăți, precum adresele de e-mail de afaceri ca prenume.numa@societate.ro sau numerele de telefon ale angajaților.

În cazul în care este necesar a fi prelucrate date cu caracter personal, acestea ar trebui să fie **adecvate, relevante și limitate la ceea ce este necesar în scopul respectiv („reducerea la minimum a datelor”)**. În calitate de operator, societatea trebuie să evalueze ce volum de date este necesar și de a se asigura că nu se colectează date irelevante.



● **Exemplu:** În cazul unei societăți care oferă persoanelor fizice servicii de închiriere a autoturismelor, se vor colecta și prelucra următoarele date: nume, adresa și numărul cardului de debit/credit al clienților și, poate, informații privind o eventuală dizabilitate de care suferă persoana în cauză (așadar, date privind sănătatea), dar nu și de originea rasială/sexul clienților.

Cui i se aplică GDPR? Este important unde are sediul o societate pentru a vedea dacă se aplică GDPR?

GDPR se aplică în cazul:

- unei societăți care prelucrează date cu caracter personal la sediul sau la sediul unei sucursale din UE sau
- unei societăți care are sediul în afara UE și oferă bunuri/servicii (contra cost sau gratuit) unor cetățeni ai unor țări membre UE sau monitorizează comportamentul unor persoane fizice din UE.

Exemplu când se aplică GDPR: O societate de recrutare cu activitate online și sediu în afara UE. Aceasta vizează în principal studenții din UE. Ea oferă consultanță gratuită cu privire la mai multe slujbe din SUA, iar studenții au nevoie de un nume de utilizator și o parolă pentru a accesa materialele online.

Exemplu când nu se aplică GDPR: O societate care este un portal de vânzare și închiriere de bunuri imobile dintr-o țară din afara UE. Societatea are sediul în afara UE și oferă servicii unor persoane din afara UE. Clienții pot utiliza aceste servicii când călătoresc în alte țări, inclusiv pe teritoriul UE. Atât timp cât serviciile prestate de societate nu se adresează în mod specific persoanelor fizice din UE, societatea nu face obiectul normelor GDPR.

Nu este relevantă dimensiunea companiei – GDPR-ul se aplică și societăților mari și societăților mici sau mijlocii (IMM) care prelucrează date conform descrierii de mai sus. Activitățile care prezintă riscuri ridicate pentru drepturile și libertățile persoanelor fizice, indiferent dacă sunt desfășurate de către un IMM sau de către o corporație, atrag aplicarea unor norme suplimentare, mai dure. Cu toate acestea, unele obligații prevăzute de GDPR nu li se aplică tuturor IMM-urilor.

De exemplu, societățile cu mai puțin de 250 de angajați nu au obligația să păstreze evidențe ale activităților lor de prelucrare decât dacă prelucrarea datelor cu caracter personal este o activitate regulată, reprezintă o amenințare la adresa drepturilor și a libertăților persoanelor fizice sau se referă la date sensibile ori la caziere judiciare.

Tot astfel, IMM-urile au obligația de a numi un responsabil cu protecția datelor numai dacă prelucrarea reprezintă activitatea lor principală și dacă aceasta implică anumite amenințări la adresa drepturilor și a libertăților persoanelor fizice (cum ar fi monitorizarea persoanelor fizice sau prelucrarea unor date sensibile ori a unor caziere judiciare), în special pentru că se desfășoară la scară largă.

Pentru a fi la curent cu prevederile legale în materie de protecție a datelor cu caracter personal, recomandăm operatorilor de date

consultarea permanentă a paginii web a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal pe următoarea adresă: <http://www.dataprotection.ro/>. La secțiunea de legislație se pot observa trei subcapitole și anume Legislație internă, Legislație UE și Decizii A.N.S.P.D.C.P.

Norme GDPR obligatorii pentru toate societățile

GDPR a stabilit o serie de principii pe care toți operatorii de date cu caracter personal ar trebui să le urmeze, textul de lege fiind scris la nivel de recomandare, urmând ca DPO-ul să ajute la interpretarea adecvată a fiecărui principiu în scopul de a se asigura de respectarea acestora în acord cu obiectul de activitate al operatorului.

Aceste principii ghidează raționamentul DPO-ului în găsirea de soluții operaționale care să ajute la buna desfășurare a prelucrării, cu respectarea drepturilor persoanelor vizate. Cu alte cuvinte, principiile sunt liniile generale de avut în vedere la începutul oricărui tip de prelucrare.

Tipul și cantitatea de date cu caracter personal pe care societatea are dreptul să le prelucereze depind de motivul pentru care sunt prelucrate (temeiul juridic în cauză) și de scopul în care sunt prelucrate. Societatea/organizația trebuie să respecte mai multe norme-cheie, inclusiv următoarele:

- datele cu caracter personal trebuie prelucrate într-un mod legal și transparent, garantând echitatea în ceea ce privește persoanele fizice ale căror date cu caracter personal sunt prelucrate („legalitate, echitate și transparență”);
- trebuie să existe scopuri specifice ale prelucrării datelor și societatea trebuie să informeze persoanele fizice în legătură cu scopurile respective atunci când le colectează date cu caracter personal. Societatea nu poate colecta pur și simplu date cu caracter personal în scopuri nedefinite;
- societatea trebuie să colecteze și să prelucereze numai acele date cu caracter personal care sunt necesare pentru îndeplinirea scopului respectiv („reducerea la minimum a datelor”);
- societatea trebuie să se asigure că datele cu caracter personal sunt exacte și actualizate, având în vedere scopurile pentru care sunt prelucrate, și să fie corectate în caz contrar („exactitate”);
- societatea nu are dreptul să utilizeze datele cu caracter personal în alte scopuri care nu sunt compatibile cu scopul inițial;
- societatea trebuie să se asigure că datele cu caracter personal nu sunt stocate mai mult timp decât este necesar pentru scopurile în care au fost colectate („limitări legate de stocare”);

- societatea trebuie să prevadă garanții tehnice și organizaționale adecvate care să asigure securitatea datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnologice adecvate („integritate și confidențialitate”).

!

- **Exemplul 1:** Un magazin online trebuie să le explice clienților săi într-un limbaj clar și simplu politica sa de confidențialitate, de ce are nevoie de datele colectate, cum le va utiliza și cât timp intenționează să le păstreze.

!

- **Exemplul 2:** O societate care organizează un târg în cadrul căruia vizitatorii se înregistrează trebuie să comunice exact către cine și care dintre date vor ajunge la societățile care sunt expozante în cadrul respectivului târg.

Ce înseamnă „prelucrare a datelor”?

Prelucrarea datelor înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

„Restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora fie în vederea criptării sau anonimizării, fie atunci când o persoană ale cărei date au fost prelucrate a solicitat acest lucru, fie în vederea ștergerii acestora atunci când se împlinește termenul pe care societatea s-a angajat să îl respecte pentru păstrarea datelor.

Scopul prelucrării datelor. Pot fi prelucrate datele în orice scop?

Nu, scopul în care sunt prelucrate datele cu caracter personal trebuie cunoscut, iar persoanele fizice ale căror date sunt prelucrate trebuie informate. Nu se poate menționa pur și simplu că se vor colecta și prelucra date cu caracter personal. Acesta este principiul „limitărilor legate de scop”. Astfel, atât în mediul online (în cadrul politicii de confidențialitate cât și în

cazul formularelor prezentate pentru diferite înscrieri/înregistrări, trebuie să fie menționat scopul pentru care se solicită acele date.

Dacă o societate a colectat date în temeiul unui consimțământ (exemplu: în scop de marketing) sau al unei cerințe legislative (exemplu: pentru emiterea unei facturi), nu este posibilă nicio prelucrare ulterioară care depășește domeniile acoperite de consimțământul inițial sau de dispoziția legislativă. Prelucrarea ulterioară ar necesita obținerea unui nou consimțământ sau un nou temei juridic. Acest lucru înseamnă că dacă o persoană a comunicat adresa sa pentru a primi prin curier ce a cumpărat de la un magazin online, respectivul magazin online nu îi va putea trimite broșuri publicitare la respectiva adresă fără a obține un consimțământ special.



Exemplu de caz când nu trebuie obținut un consimțământ suplimentar: Un IFN are un contract cu un client pentru a-i oferi clientului un împrumut de nevoi personale. La sfârșitul primului an, IFN-ul utilizează datele cu caracter personal ale clientului pentru a verifica dacă acesta este eligibil pentru un tip de împrumut mai avantajos. În acest caz, IFN-ul trebuie doar să informeze clientul și nu trebuie să îi obțină consimțământul.

Dar dacă IFN-ul dorește să transmită datele clientului unor firme de asigurări, în temeiul aceluiași contract pentru acordarea unui împrumut, acesta nu va putea prelucra fără consimțământul explicit al clientului, deoarece scopul nu este compatibil cu scopul inițial în care au fost prelucrate datele.

Cât timp pot fi păstrate datele? Se impune actualizarea lor?

Datele trebuie să fie stocate pentru o perioadă cât mai scurtă posibil. Perioada ar trebui să țină seama de motivele pentru care societatea trebuie să prelucreze datele, precum și de eventuale obligații de a păstra datele o perioadă fixă de timp (de exemplu sunt anumite legi care instituie o obligație legală pentru păstrarea documentelor cum ar fi legislația din domeniul dreptului muncii, legislația fiscală sau legile antifraudă sau împotriva spălării banilor care impun păstrarea datelor cu caracter personal ale angajaților pentru o perioadă determinată).

Fiecare societate ar trebui să stabilească termene pentru ștergerea sau revizuirea datelor stocate (redactând politici de retenție a datelor – vom discuta despre aceste politici în capitolele următoare).

Ca excepție, datele cu caracter personal pot fi păstrate o perioadă mai îndelungată în scopuri de arhivare în interes public ori în scopuri de

cercetare științifică sau istorică, cu condiția să fie puse în aplicare măsuri de ordin tehnic și organizatoric adecvate (precum anonimizare, criptare etc.).

!

● **Exemplu:** Cât timp ar trebui să păstreze o agenție de turism datele clienților săi? Este în regulă să le păstrați timp de 20 de ani? Perioada de stocare nu pare proporțională cu scopul de a găsi vacanța potrivită pe termen scurt până la mediu. În acest caz societatea ar trebui să își facă un plan și apoi să solicite clienților acordul pentru a trimite informații despre noi destinații, având grijă să păstreze și să prelucereze datele doar perioada de timp comunicată.

Principiile de bază ale GDPR

Societățile care colectează și procesează date personale sunt obligate să implementeze și să aplice cu strictețe prevederile GDPR, respectând 7 principii de bază:

1. Legalitate, echitate și transparență. Acesta este un principiu esențial, strâns asociat cu drepturile fundamentale ale omului. Datele cu caracter personal trebuie să fie prelucrate *„în mod legal, echitabil și transparent față de persoana vizată.”*

2. Principiul limitării scopului. Aceasta impune ca datele cu caracter personal să fie colectate numai în scopuri specificate, explicite și legitime.

3. Reducerea la minimum a datelor colectate. Astfel, datele colectate trebuie să fie adecvate, limitate și relevante. Prin acest principiu operatorii sunt avizați de faptul că orice colectare de date personale trebuie foarte bine analizată înainte de obținerea efectivă a datelor, care trebuie să fie cele mai relevante și strict limitate la ceea ce este absolut necesar pentru scopurile în care sunt prelucrate.

Societatea nu trebuie să păstreze mai multe date personale decât are nevoie pentru a-și atinge scopul. De asemenea, datele nu trebuie să cuprindă detalii irelevante.

Dacă un manager decide (sau pur și simplu uită să verifice) să păstreze mai multe date decât este necesar pentru scopul pe care îl are (deoarece majoritatea bazelor legale au elementul necesității), încalcă principiul minimizării datelor și persoanele vizate vor avea dreptul de a solicita ștergerea lor.

4. Principiul menținerii datelor actualizate asigură faptul că datele cu caracter personal sunt corecte și sunt actualizate acolo unde este necesar.

5. Principiul stocării datelor strict pe perioada pentru care s-a obținut consimțământul. Acesta presupune ca datele cu caracter personal să fie păstrate într-o formă care să permită identificarea persoanelor vizate cel mult timp necesar pentru prelucrarea datelor.

6. Principiul asigurării securității adecvate datelor astfel încât acestea să fie integre, confidențiale și disponibile.

7. Principiul responsabilității. Societatea este responsabilă de respectarea principiilor enumerate la art. 5 alin. (1) din GDPR și trebuie să fie în măsură să demonstreze respectarea acestora.

Prelucrarea datelor personale trebuie făcută în cele mai proprii condiții de siguranță, care să includă „protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare” (o modalitate recomandabilă pentru asigurarea respectării condițiilor de siguranță este obținerea certificării ISO 27001).

Este important de reținut faptul că societatea trebuie să fie în măsură să demonstreze în orice moment respectarea acestor principii.

Există dispoziții specifice pentru datele referitoare la copii?

GDPR afirmă explicit că datele personale ale copiilor merită o protecție specifică.

În ceea ce privește oferirea de servicii în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puțin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului. Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.

● **Exemplu:** O școală de dans sportiv pentru copii va colecta și prelucra date referitoare la sănătatea cursanților numai cu acordul părinților.

În ceea ce privește societățile care funcționează în mediul online, acestea trebuie să depună eforturi rezonabile, ținând seama de tehnologiile disponibile, pentru a se asigura că respectivul consimțământ a fost într-adevăr acordat în conformitate cu prevederile legii. Cu alte cuvinte,

societatea trebuie să pună în aplicare măsuri de verificare a vârstei (ex: întrebări de control, acțiuni efectuate pe site-ul web etc.).

În plus, în acest caz, trebuie ca societatea să se asigure că informațiile și comunicările sunt ușor accesibile și sunt exprimate într-un limbaj simplu și clar, astfel încât copilul să îl poată înțelege cu ușurință.

Când colectarea datelor se referă în special la date ale unor minori, trebuie stabilit în primul rând temeiul (legal, contractual/consimțământ). Dacă ne raportăm la consimțământ ca temei pentru prelucrare, atunci copilul trebuie să poată înțelege ceea ce acceptă, altfel consimțământul nu este „informat” și, prin urmare, nu este valabil. Există și câteva reguli suplimentare pentru consimțământul online. Dacă temeiul este contractual (în vederea încheierii unui contract), atunci trebuie luată în considerare capacitatea copilului de a accepta contractul și de a înțelege implicațiile prelucrării. Dacă temeiul este interesul legitim, trebuie ca societatea să echilibreze propriile interese legitime cu drepturile și libertățile fundamentale ale copilului. Aceasta implică o verificare în ceea ce privește natura și scopul prelucrării și riscurile potențiale pentru copii.

Cel mai important de reținut, societatea trebuie să se asigure că de fiecare dată sunt luate măsurile adecvate pentru a proteja copiii împotriva oricăror riscuri.

!

● **Exemplu:** Dacă o societate furnizează jocuri gratuite pentru copii online, ar trebui să obțină consimțământul părintelui sau al tutorelui, întrucât nu va fi evidentă vârsta copiilor care vor accesa jocurile respective.

Dacă prelucrarea de date ale minorilor este susceptibilă să ducă la un risc ridicat pentru drepturile și libertățile copiilor, atunci trebuie să faceți o DPIA (o evaluare a impactului protecției datelor). Lista prelucrărilor susceptibile să genereze un risc pentru persoanele vizate și care necesită o DPIA include utilizarea datelor personale ale copiilor în scopuri de marketing, profilare sau alte decizii automatizate sau dacă se intenționează oferirea de servicii online direct copiilor – vom discuta mai pe larg despre aceste DPIA în capitolele următoare.

Rețelele sociale precum Facebook sau serviciile de cotație financiară sunt exemple de organizații care oferă servicii ale societății informaționale.

Considerentul 38 al GDPR explică de ce este atât de important pentru aceste tipuri de organizații să stabilească vârsta utilizatorilor lor: „Copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal.”

Această protecție specifică ar trebui să se aplice în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator și la colectarea datelor cu caracter personal privind copiii în momentul utilizării serviciilor oferite direct copiilor. Consimțământul titularului răspunderii părintești nu ar trebui să fie necesar în contextul serviciilor de prevenire sau consiliere oferite direct copiilor”.

Măsuri tehnice și organizatorice

Un principiu important al GDPR-ului este acela al prelucrării securizate, principiu care se referă la adoptarea unui set de măsuri tehnice și organizatorice menite să protejeze datele cu caracter personal ale persoanelor vizate.

Operatorii de date au responsabilitatea de a asigura controlul și protecția datelor într-un cadru organizat și controlat, care să permită respectarea drepturilor persoanelor vizate în timpul prelucrării. Măsurile tehnice și organizatorice puse în aplicare de societatea/instituția în cauză (operator) impun elaborarea unui plan adecvat, pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul.

Exemple de măsuri tehnice și organizatorice:

1. Informarea/școlarizarea utilizatorilor (training-uri care trebuie ținute frecvent în cadrul companiei);
2. Managementul identității și accesului (accesul în interiorul unei clădiri, accesul în rețeaua sistemului informatic sau accesul în interiorul unei aplicații din cadrul organizației)
3. Securitatea stațiilor de lucru;
4. Securitatea rețelei interne;
5. Asigurarea continuității procesării informației (efectuarea unor backup-uri, precum și testarea periodică a acestora, implementarea unui plan de continuitate a business-ului în cazul pierderii informațiilor);
6. Managementul procesatorilor (informațiile și datele transferate în vederea prelucrării către terțe organizații colaboratoare, trebuie să fie de asemenea protejate în mod corespunzător);
7. Securitatea fizică a societății (instalarea de sisteme de supraveghere video (CCTV), utilizarea de sisteme de autentificare a angajaților (carduri de acces, pin etc.), implementarea unei politici privind vizitatorii din cadrul organizației;

8. Stabilirea de proceduri privind securitatea datelor și informarea tuturor angajaților cu privire la respectarea acestora;

9. Stabilirea în cadrul societății a unui Responsabil de date cu caracter personal (intern – angajat sau extern – colaborator care să urmărească activitatea fiecărui departament și implementarea în cadrul acestora a procedurilor menționate la **punctul 8**).

BUNE PRATICI ÎN MANAGEMENTUL ȘI ADMINISTRAREA COMPANIEI

*„Ți-ai construit castele în aer? Bine, chiar acolo trebuie clădite.
Acum, mergi la lucru și construiește fundația sub acestea.”*

Henry David Thoreau

Obiectivul principal al oricărei afaceri este profitul, acesta fiind și motivul pentru care, de cele mai multe ori, antreprenorii văd societatea ca un lucru „rezolvat” odată cu obținerea CUI-ului de la Registrul Comerțului și de acolo încep să se preocupe doar de serviciile și produsele pe care abia așteaptă să le ofere clienților lor conform unui plan prestabilit.

Nu este nimic greșit în această abordare, exceptând faptul că lipsa de informare de la bază poate crea probleme majore business-ului în momentele cel mai puțin așteptate și de regulă când nu există timp, echipă sau buget cu care să remediezi situația. De aceea, cade în sarcina administratorului să țină cont de toate normele în vigoare de la momentul constituirii societății și să se asigure de integrarea lor corespunzătoare încă de la început.

Pe lângă norme de fiscalitate, siguranță și securitate în muncă, protecția mediului înconjurător sau alte autorizații specifice companiei, GDPR este un alt set de reguli de care trebuie să se țină cont încă de la fondarea societății.

Implementarea clauzelor GDPR în actul constitutiv al firmei și în AGA

În funcție de forma de organizare a unei societăți urmează ca administrarea acesteia să se realizeze prin organele ei de conducere care pot fi, după caz, administratorii, directorii generali, consiliul de administrație sau chiar președintele. În toate cazurile, încă de la înființarea societății prin redactarea actului constitutiv trebuie să se țină cont de o serie de împrejurări care sunt veritabile prelucrări de date cu caracter personal ale persoanelor implicate.

În concret, orice societate formată din minimum un asociat urmează să angajeze firma în relații cu terți, de la furnizorii de servicii, la clienți, sau

autorități acesta fiind și motivul pentru care încă de la înființare se vor avea în vedere normele GDPR care stabilesc responsabilitatea operatorului potrivit cerințelor stabilite de lege. De aceea, pe lângă clauzele obișnuite pe care le conține actul constitutiv, trebuie să se stabilească cel puțin câteva dintre scopurile prelucrărilor de date pe care le va realiza societatea în derularea activității precum și principiile de prelucrare în ceea ce privește datele persoanelor implicate în mod direct în activitatea societății.

În cazul firmelor conduse de mai mult de o persoană, se vor avea în vedere situațiile în care părțile implicate vor avea acces la datele personale ale terților, prelucrate în procesele de business, la datele salariiților sau ale rudelor acestora și în schema de implementare trebuie să se țină cont de activitatea de prelucrare realizată de operator, obiectul de activitate al operatorului, structura activității economice, precum și structura organizatorică a societății.

Exemplu: În cazul unei societăți cu obiect de activitate în domeniul pazei și protecției asupra bunurilor și persoanelor se impune ca operatorul să aibă în vedere că, prin însăși natura serviciilor prestate, va prelucra date cu caracter personal multiple cu care se va intra în contact pe mai multe niveluri: angajații companiei în furnizarea serviciului, organele de cercetare penală în baza Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor precum și a Codului penal, administrația companiei pentru a lua decizii, furnizorii de echipamente pentru supraveghere în calitate de împuterniciți ai operatorului etc.

De aceea, în actul constitutiv al societății, față de codurile CAEN autorizate, operatorul trebuie să stabilească, cel puțin la nivel principal, responsabilitatea în raport cu dispozițiile GDPR și să se asigure că accesul la datele cu caracter personal prelucrate se va realiza pe niveluri, în urma unei analize amănunțite, pentru a nu aduce atingere drepturilor și libertăților fundamentale ale persoanelor vizate, obiect al prelucrării.

Ca principiu, în orice societate trebuie să existe acces limitat la anumite categorii de date cu caracter personal în funcție de natura lor, de scopul prelucrării și de riscurile la care pot fi supuse persoanele vizate în concordanță cu sectorul de activitate în care se realizează prelucrarea.

Un alt aspect care se va avea în vedere este structura administrativ teritorială a societății întrucât pot exista situații în care una sau mai multe persoane care fac parte din conducerea societății sau, după caz, a consiliului de administrație se pot situa fizic într-un alt oraș, într-un alt stat sau chiar într-un alt stat non-membru UE și astfel clauzele GDPR se vor aplica împreună cu stabilirea unor garanții suficiente care să completeze măsurile

de securitate în ceea ce privește transferul de date personale către organul de conducere din afara spațiului european. Aceleași preocupări trebuie să existe și în cazul în care, în structura administrativă, sunt implicate persoane fizice sau juridice de altă cetățenie, non-membre UE, către care transferul de date se va realiza cu ocazia raportărilor situațiilor financiare sau transmiterii altor rapoarte ale directoratului la care asociații au acces în baza Legii nr. 31/1990 privind societățile comerciale.

Astfel, deși dispozițiile legale în vigoare stabilesc reguli clare cu privire la dezvăluirea anumitor informații, în cazul societăților pe acțiuni existând chiar și posibilitatea publicării anumitor date personale pe pagina de internet a societății⁶, totuși, actul constitutiv este cel care poate stabili de la bun început limitarea dezvăluirii datelor cu caracter personal la cele necesare.

„Când actul constitutiv nu dispune altfel, ele se vor ține la sediul societății și în locul ce se va indica în convocare, (1) Situațiile financiare anuale, raportul anual al consiliului de administrație, respectiv raportul directoratului și cel al consiliului de supraveghere, precum și propunerea cu privire la distribuirea de dividende și situația privind dividendele distribuite parțial în cursul anului fiscal se pun la dispoziția acționarilor la sediul societății, de la data convocării adunării generale. La cerere, acționarilor li se eliberează copii ale acestor documente. [...] (2) În cazul în care societatea deține o pagină de internet proprie, convocarea, orice alt punct adăugat pe ordinea de zi la cererea acționarilor, în conformitate cu art. 117¹, precum și documentele prevăzute la alin. (1) se publică și pe pagina de internet, pentru liberul acces al acționarilor. (3) Fiecare acționar poate adresa consiliului de administrație, respectiv directoratului, întrebări în scris referitoare la activitatea societății, înaintea datei de desfășurare a adunării generale, urmând a i se răspunde în cadrul adunării.”

Actul constitutiv redactat la înființarea societății poate suferi modificări pe parcursul desfășurării activității economice a firmei, acesta fiind și motivul pentru care una dintre recomandările pentru operatorii de date este de a ține cont că orice modificare intervine în societate, care ar putea conduce implicit la o modificare de act constitutiv, să îl revizuiască și din perspectiva implementării normelor GDPR, putând stipula acele reguli privind prelucrarea de date care să ajute la respectarea principiilor minimizării și a limitării la scop.

⁶ Art. 110 alin. (2), art. 1171, art. 1172 din Legea nr. 31/1990.

Adunarea Generală a Asociaților

În cadrul adunărilor generale ale asociațiilor se pot dezvălui mai multe categorii de date cu caracter personal în scopul luării anumitor decizii necesare bunei desfășurări a activității societății. În cazurile cu grad de risc ridicat, este necesar ca operatorul, prin persoana care conduce adunarea, să stabilească un cadru de siguranță pentru persoanele vizate ce fac obiectul prelucrării.

! **Exemplu:** Într-o societate în care a fost înregistrat video un caz de furt semnificativ prin existența unor camere de supraveghere instalate în edificiu cu scopul precis de a monitoriza siguranța mărfii care se regăsea în locația specifică, se deschide într-o adunare generală subiectul suplimentării cu pază umană pentru sporirea siguranței. Buna practică în gestionarea unei astfel de situații este declarația verbală sau scrisă a persoanei direct responsabile cu supravegherea video, nicidecum rularea imaginilor care conțin date biometrice privind trăsăturile fizionomice ale persoanei vizate care a săvârșit infracțiunea, indiferent de faptul că respectiva persoană este un angajat al societății. Imaginile pot fi dezvăluite doar organelor de cercetare penală care vor fi implicate în luarea măsurilor legale care se impun.

Pentru respectarea clauzelor GDPR, administratorii trebuie să se asigure de faptul că în cadrul adunărilor generale nu se vor dezvălui decât acele date cu caracter personal necesare dezbaterii punctelor de pe ordinea de zi, cu respectarea principiilor de actualitate, necesitate, minimizare și limitare la scop. Deși apare ca natural în discuțiile dintre asociați să dezbată inclusiv probleme familiale ale anumitor salariați din cadrul companiei, întotdeauna se va ține cont de faptul că, în afara scopurilor pentru care există un temei legal sau contractual, angajații trebuie să își dea consimțământul expres pentru respectiva prelucrare, în afara cazului în care nu poate fi invocat un interes legitim al operatorului.

În toate cazurile, se recomandă ca ședințele ce au ca obiect adunări generale de asociați să țină seama din deschidere de responsabilitatea pe care o are operatorul față de datele prelucrate în diferite scopuri stabilite de respectiva adunare, luând în considerare și acele decizii care sunt publicate pe platforme online care vor dezvălui datele persoanelor vizate față de un număr de vizitatori nelimitat. Identificarea persoanelor vizate din procesele verbale, atât nepublice, cât și publice, se va face printr-un număr minim de date personale, doar cele necesare, fără a fi conținute detalii suplimentare fără un scop legal, cum ar fi CNP-ul sau adresa de domiciliu.

Nu în ultimul rând, în redactarea actelor specifice pentru a fi depuse la Registrul Comerțului, se va ține cont de același principiu de a consemna doar acele date necesare și utile scopului lor întrucât unele decizii de administrație se publică inclusiv în Monitorul Oficial al României prin acesta devenind publice. Inclusiv cesiunile de părți sociale care au în vedere cooptarea în firmă a unui asociat nou se publică în Monitorul Oficial, iar pentru acest motiv trebuie să existe o responsabilitate și o diligență sporită în alegerea tipurilor de date cu caracter personal care se consemnează în documente. Indiferent dacă vorbim de documente care se publică sau care rămân doar la dosarul ținut de Registrul Comerțului, se va respecta același principiu al minimizării prevăzut de GDPR pentru că orice persoană care justifică un interes poate face o cerere pentru eliberarea unor documente de la dosar, nefiind așadar securizate total în nicio situație.

Implicarea administratorului în luarea măsurilor tehnice și organizatorice și în monitorizarea lor. Numirea unui DPO/DPC

Administratorul societății este prima persoană care trebuie să se familiarizeze cu principiile GDPR, să se informeze în legătură cu responsabilitățile pe care le are firma în calitate sa de operator de date cu caracter personal față de angajați, față de terți furnizori, parteneri de afaceri, clienți, și nu în ultimul rând, față de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal sau alte autorități europene cu același specific.

Dacă înainte de intrarea în vigoare a Regulamentului, operatorul de date cu caracter personal era doar entitatea care prelucra datele unor persoane vizate în vederea îndeplinirii scopului economic, sau pentru marketing și vânzări, astăzi operator este orice firmă mică ce activează în online sau offline chiar dacă are un singur salariat, sau nu are deloc.

Astfel, administratorul societății trebuie să fie implicat în mod direct în procesul decizional în ceea ce privește implementarea normelor GDPR, fie personal, fie printr-un reprezentant numit.

Sunt două situații cu care se poate confrunta o companie, cea în care, dat fiind fluxul de date, numărul de angajați, mărimea acesteia și obiectul de activitate, nu se impune numirea unui responsabil cu protecția datelor și cea în care se recomandă o astfel de persoană desemnată pentru a răspunde rigorilor stabilite de Regulament și ghidurile emise de Comitetul European pentru Protecția Datelor.

Pe site-ul autorității din UK există o secțiune⁷ dedicată pentru orice societate care nu poate stabili dacă este sau nu este necesară numirea unui DPO, de tipul unui chestionar prin care în urma răspunsurilor la 3 întrebări simple orice firmă poate stabili dacă este sau nu este necesară numirea unui responsabil cu protecția datelor.

Pentru a vă ajuta să treceți prin aceste întrebări și a stabili împreună acest aspect, regăsiți mai jos cele trei întrebări fundamentale:

1. Sunteți sau nu o autoritate publică?
2. Activitatea de bază a societății dumneavoastră este prelucrarea sistematică și monitorizarea persoanelor vizate pe scară largă?
3. Prelucrați ca activitate de bază categorii de date speciale sau date privind condamnări penale ale persoanelor vizate?

la care am mai putea adăuga întrebarea cu numărul 4: Aveți peste 250 de salariați?

Dacă răspunsul la oricare dintre aceste întrebări cu excepția primeia este DA, atunci se recomandă numirea unui Data Protection Officer – DPO, autoritățile publice fiind obligate prin lege să numească unul.

O alternativă la numirea unui DPO este optarea către un DPC – Data Protection Counsel – un consultant specialist pe protecția datelor care poate să vă sfătuiască în ceea ce privește implementarea GDPR și să monitorizeze activitatea firmei periodic.

Indiferent pentru care dintre variante veți opta sau, dacă nu este cazul, nu veți opta pentru niciuna, totuși conformarea inițială este necesară, dat fiind faptul că riscul la care se supune societate este unul foarte ridicat. Dacă în cazul altor tipuri de plângeri la care este supusă o societate, persoanele care pot face sesizarea sunt de obicei dintr-o anumită categorie, spre exemplu, un salariat poate face plângere la ITM, un client nemulțumit la protecția consumatorilor și tot așa, în cazul încălcărilor GDPR, persoana vizată poate fi din orice categorie și expunerea firmei este mult mai mare. Așadar, administratorul societății trebuie să decidă asupra alocării unui buget pentru implementarea GDPR și, dacă este cazul, numirii unui DPO, acest lucru fiind necesar încă de la început, pentru a avea un specialist care să îl țină la curent cu bunele practici în cadrul companiei.

În cazul în care potrivit ghidurilor și recomandărilor pe care le avem de la autoritățile competente pe protecția datelor, rezultă că este necesară numirea unui DPO, administratorul nu poate îndeplini această funcție, ci trebuie să numească o altă persoană din cadrul companiei sau să

⁷ <https://ico.org.uk/for-organisations/does-my-organisation-need-a-data-protection-officer-dpo/>.

externalizeze serviciul. Incompatibilitatea administratorului cu funcția de DPO este o măsură de siguranță pe care o ia GDPR, pentru a evita îndeplinirea doar formală a acestei funcții.

Un grup de firme poate numi un DPO comun, dacă structura organizatorică și dimensiunea societăților permit acest lucru.



Exemplu „AȘA NU!”: Numirea șefului departamentului financiar-contabil ca DPO poate conduce la influențarea deciziilor privind implementarea unei măsuri tehnice costisitoare pe motivul că bugetul nu permite alocarea unei sume de bani considerabile și pentru că este persona care se implică direct alături de administrator în stabilirea acestuia. Din rațiuni economice, poate stabili că este mai bine să evite implementarea unui ISO care este absolut necesar. De asemenea, nu are o legătură directă cu toate celelalte departamente și comunicarea cu colegii este lacunară.



Exemplu „AȘA DA!”: Assistant managerul este o persoană potrivită, pentru că poate fi instruită în domeniul protecției datelor, nu ia decizii privind bugetele și propune măsuri având legătură cu toate departamentele societății. Acesta poate, împreună cu administratorul, să creeze fluxul corect de date și să se implice și în monitorizarea respectării normelor.

Regula de bază în atingerea unei implementări eficiente este comunicarea proactivă între managementul societății și DPO. Acest lucru se poate realiza și dacă este vorba despre o persoană numită din cadrul societății, dar și în cazul externalizării serviciului către un terț specializat.

Avantajul în numirea unui DPO extern este acela că la baza raportului juridic stă un contract de furnizare servicii în cadrul căruia se stabilesc drepturile și obligațiile părților și poate avea o durată nedeterminată, contra unui preț. Firmele specializate pe astfel de servicii oferă expertiză extinsă pentru tot ce presupune aplicarea bunelor practici în domeniul protecției datelor cu caracter personal și pot aduce un plus prin formarea unor echipe de mai mult de o persoană care să se ocupe de implementare și ulterior de monitorizare.

În cazul numirii unei persoane din interiorul companiei, avantajul este că administratorul are acces direct la salariat, însă pregătirea acestuia presupune anumite investiții financiare, iar stabilitatea este tot timpul sub

semnul întrebării. Sarcinile angajatului care ocupă funcția de DPO se stabilesc prin fișa de post, anexă la contractul individual de muncă.

Practica a mai dovedit un aspect esențial pe care administratorii ar trebui să îl ia în calcul atunci când decid asupra numirii unui DPO intern, anume că, în cele mai multe dintre situații, salariatul nu a gestionat în mod potrivit sarcinile atribuite ca DPO, având de realizat și munca sa recurentă, potrivit postului principal pe care îl ocupă. Lipsa de timp în realizarea unui studiu de impact, să zicem, poate conduce la inițierea unui proces nou de prelucrare în cadrul companiei care nu a fost analizat în prealabil din punct de vedere al riscurilor și care poate produce pagube în viitor. Conform paragrafelor din GDPR care stabilesc responsabilitățile DPO, acesta nu poate fi demis sau sancționat pentru îndeplinirea sarcinilor sale, drept urmare, dacă apare o situație care prejudiciază compania, nu se pot lua niciun fel de măsuri împotriva salariatului.

Monitorizarea măsurilor tehnice și organizatorice

Orice sistem adoptat trebuie să fie verificat periodic. În cazul efectuării unei implementări GDPR într-o societate, monitorizarea existenței și respectării măsurilor este esențială pentru o protecție adecvată a persoanelor vizate în primul rând și a operatorului de date în al doilea.

În ce constă monitorizarea? În cazul măsurilor organizatorice se referă la un check-list al cunoașterii de către persoanele care le aplică la o perioadă de timp rezonabilă, recomandat lunar sau maxim din 3 în 3 luni. În cazul măsurilor tehnice monitorizarea constă în verificarea funcționalității și eficienței lor, în mod similar, lunar sau periodic, în funcție de mecanisme. Dacă situația practică o impune, sau există suspiciunea unei breșe de securitate, monitorizarea se va face de fiecare dată când se va dovedi necesar.

Precizăm că, în cazul verificării aplicării măsurilor organizatorice de către toate persoanele din societate, este necesară implicarea șefilor de departamente pentru a facilita administratorului și responsabilului cu protecția datelor comunicarea cu salariații.

Activități care ajută la monitorizarea măsurilor organizatorice:

- aplicarea unui test de cunoștințe angajaților cu acces direct la date care să măsoare gradul de înțelegere a noțiunilor GDPR și a impactului asupra companiei;
- încurajarea tuturor salariaților să trimită noutăți legate de schimbările care pot apărea pe parcursul activității societății raportat la diferite tipuri de date prelucrate;

- simularea unui control la nivel de departament;
- ședințe deschise și training-uri periodice pe tema datelor cu caracter personal.

Lipsa monitorizării poate lipsi de eficiență orice tip de măsură implementată și supune operatorul de date la riscuri majore.



Exemplu „AȘA NUI”: Copierea unor proceduri GDPR de la alte societăți fără aplicarea concretă la nivelul operatorului în discuție sau utilizarea unor proceduri standard care nu au nicio legătură cu domeniul de activitate al companiei, fără a avea în vedere verificarea utilității practice. Se constată astfel, că nu poate exista un plan de monitorizare dacă nu există implicare din partea administratorului în implementarea coerentă a normelor specifice în compania sa.



Exemplu „AȘA DA!”: Abonarea la un portal de noutăți legislative specifice sau afilierea la o organizație cu preocupări în domeniu care să contribuie permanent la actualizarea noțiunilor pe baza cărora se construiesc politicile GDPR din companie.

Cooperarea între administrația societății și DPO/DPC

Responsabilul cu protecția datelor trebuie să facă eforturi constante pentru a coordona întreaga activitate de prelucrare de date a unei societăți și să se asigure că prezintă date clare și informații esențiale administratorului companiei. Acesta din urmă nu trebuie decât să aprobe deciziile DPO-ului care propune măsurile tehnice și organizatorice pe care firma trebuie să le implementeze și să le monitorizeze.

Un aspect important în comunicarea cu administratorul este stabilirea unor ședințe cu o anumită regularitate și prezentarea situației la zi, iar atunci când se impune, stabilirea unor ședințe de urgență care pot avea în componență și șefi de departamente sau alte persoane cheie din interiorul companiei. Astfel de ședințe sunt necesare ori de câte ori apare o prelucrare nouă de date, spre exemplu organizarea unui concurs sau a unei loterii publicitare, atunci când pleacă din companie un salariat cu acces nelimitat la anumite categorii de date cu caracter personal, pentru a se asigura de gestiunea corectă a situației și asigurarea unei securități potrivite persoanelor vizate, sau în alte cazuri concrete care necesită decizii și responsabilitate din partea operatorului.

Atitudinea administratorului trebuie să fie de preocupare, deschidere și înțelegere față de măsurile pe care DPO-ul le propune și să nu intervină decât prin susținerea acestuia din punct de vedere logistic și financiar. Nu este corectă abordarea potrivit căreia sarcinile sunt alocate către DPO și administratorul se retrage complet din ecuația implementării, deoarece, potrivit procedurilor privind investigațiile autorității competente în domeniul protecției datelor, în cazul unui control, reprezentantul legal are un rol deosebit de important în derularea investigației și este ideal să fie la curent cu tot ce se petrece în societate pentru a putea coopera.

În cazul în care societatea face parte dintr-un grup de firme care are un DPO general numit, legătura cu acesta trebuie să fie periodică, iar comunicarea proactivă, iar nu reactivă.

Deși există un plan de implementare și monitorizare la nivel de grup, este necesar ca firma din România să țină cont de legislația specifică și de particularitățile ei și să alinieze orice politică pe verticală, primită de la conducerea grupului, în concordanță cu necesitățile naționale și particularitățile socio-politice de pe plan local.

Numirea unui DPO poate fi una dintre principalele măsuri organizatorice pe care trebuie să le ia operatorul de date cu caracter personal. Conform rapoartelor date de autoritățile de supraveghere din Europa de-a lungul ultimilor 2 ani de la intrarea în vigoare a Regulamentului, lipsa măsurilor tehnice și organizatorice a fost sancționată cu amenzi de la 2.000 de euro la 900.000 de euro, cum a fost cazul unei companii din Olanda⁸. Potrivit acestor date, trebuie tratată cu seriozitate adoptarea acestor măsuri și trebuie analizată oportunitatea numirii unui DPO, chiar dacă nu apare ca o obligație, ci mai curând o recomandare fermă.

În cazul Germaniei, o firmă privată (Rapidata GmbH) a primit o amendă de 10.000 de euro chiar pentru lipsa numirii unui DPO conform obligațiilor impuse de art. 37 din GDPR, iar Facebook Germania a primit amenda în valoare de 51.000 de euro pentru același motiv:

„Deși Facebook Irlanda a numit un ofițer de protecție a datelor pentru toate companiile din grupul din UE, această cerere nu a fost notificată DPA Hamburg, competență pentru Facebook Germany GmbH. Amenda a fost calculată pe baza cifrei de afaceri a sucursalei germane (35 de milioane EUR). Factorii relevanți pentru calcul au fost că notificarea omisă a fost imediat făcută, Facebook acționând neglijent și nu a încălcat obligația de a numi un agent de protecție a datelor, ci doar obligația de notificare⁹”.

⁸ <https://autoriteitpersoonsgegevens.nl/en>.

⁹ https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf.

Din exemplul precedent, desprindem ideea că, atunci când GDPR impune numirea unui DPO, operatorul trebuie să se subscrie și obligației de a transmite o notificare a acestuia la autoritatea de supraveghere din statul respectiv. În cazul României, notificarea va fi transmisă prin utilizarea formularului cu privire la desemnarea responsabilului privind protecția datelor cu caracter personal pe care îl regăsiți în secțiunea dedicată de pe site-ul A.N.S.P.D.C.P. www.dataprotection.ro, în partea stânga.

Așadar, administratorul societății trebuie să vadă ca o prioritate numirea unui DPO, să se asigure de notificarea acestuia la autoritate și ulterior să coopereze cu acesta în realizarea obiectivelor firmei, fără a interveni în activitatea acestuia și fără a se confunda activitățile întreprinse de conducere și de către responsabilul cu protecția datelor.

GDPR și controalele de la autoritățile publice. Registrul unic de control

În România există un număr de peste 100 de autorități centrale diferite și alte câteva sute de direcții descentralizate pe județe, potrivit datelor furnizate de Guvernul României pe site-ul său public www.gov.ro.

Controalele din partea autorităților se realizează pe nenumărate domenii, de la verificarea protecției și sănătății în muncă și până la controale sanitar-veterinare, protecția împotriva incendiilor ș.a.m.d.

Responsabilitatea operatorilor de date cu caracter personal este să identifice ori de câte ori sunt supuși unui control dacă este cazul să prezinte anumite documente din partea societății și de câte feluri sunt acestea. În funcție de autoritatea în discuție documentele supuse verificărilor sunt diferite și pot conține mai multe categorii de date cu caracter personal, fie ale angajaților, fie ale colaboratorilor, furnizorilor de servicii, sau alte înregistrări ce țin de funcționarea societății.

Potrivit GDPR, prelucrarea unor date cu caracter personal se realizează în temeiul legii și fiecare dintre autoritățile care efectuează un control are prerogativa de a verifica anumite documente tot în baza legii sau a unor norme și metodologii interne care stabilesc exact cadrul în care se realizează investigația.

Cu toate acestea, tendința administratorilor și, în special, a reprezentanților desemnați să coopereze cu organismele de control este de a pune la dispoziție mai multe documente decât cele necesare sau de a permite accesul în toate spațiile și locurile de depozitare, chiar și atunci

când nu este necesar. Plecând de la acest principiu, operatorul trebuie să se asigure de faptul că angajații săi cunosc regulile de control atunci când intervine o astfel de situație și stabilesc împreună limitele în care trebuie să dezvăluie anumite date cu caracter personal pentru a nu încălca principiile GDPR.

În concret, la nivel de companie, în procedurile interne de confidențialitate, trebuie să existe un capitol dedicat inclusiv felului în care se manifestă reprezentanții firmei în cazul unui control.

! **Exemplu de bune practici:** Organele de control vor fi primite întotdeauna într-un spațiu neutru de genul unei săli de ședință în care nu se regăsesc documente ale firmei și doar la solicitarea acestora și în baza verificării întinderii mandatului, urmează să fie poftite într-un birou sau în arhiva societății. Se vor prezenta doar acele documente solicitate care vizează obiectul controlului și, pe cât posibil, vor fi anonimizate sau pseudonimizate datele persoanelor vizate care se regăsesc pe documente, dacă scopul controlului nu este de a le verifica întocmai pe acestea. Nu se vor prezenta detalii suplimentare legate de aspecte ce țin de viața privată a salariaților, cazuri cu care s-au confruntat și care implică date sensibile precum starea de sănătate, situația familială sau detalii din cazierile fiscale ale acestora, în afara cazului în care a existat un studiu de impact anterior.

Organizarea și gestiunea documentelor în cadrul companiei nu trebuie să fie aleatorii pentru a supune firma la riscul încălcării normelor în domeniul GDPR. Atunci când sunt dezvăluite date care nu sunt necesare se poate considera că se produce o veritabilă breșă de securitate. Din acest motiv, ori de câte ori va fi necesar, va trebui să existe o preocupare în ceea ce privește felul în care se păstrează documentele, în ce spații, cine poate avea acces neautorizat la ele și dacă există măsuri de securitate suficiente care să ofere o protecție adecvată persoanelor vizate.

Această regulă trebuie păstrată indiferent dacă este vorba despre sediul principal al societății sau de punctele de lucru unde există documente sau arhive care conțin documente. Pentru că arhivele sunt comune de cele mai multe ori și nu există o separare pe categorii de documente decât prin diferențierea prin rafturi, persoanele angajate ale societății care au responsabilitatea de a permite accesul trebuie să fie instruite conform normelor GDPR și să se asigure că nu încalcă principiile de confidențialitate.



Exemplu „AȘA NU!”: În cazul unui control de la Autoritatea Națională Pentru Protecția Consumatorilor intervenit ca urmare a unei plângeri, se prezintă lista de clienți sau comenzile anterioare ale consumatorului și corespondența cu acesta deși nu a fost solicitată de către organele de control.

De asemenea, în cazul efectuării unui control, există posibilitatea ca persoanele împuternicite de autoritate să solicite inclusiv copii de pe anumite documente pe care să le ia la plecare. Doar în anumite situații extrem de particulare există un temei legal pentru această conduită, iar reprezentantul firmei controlate trebuie să se asigure că este unul dintre cazurile legale și că nu permite o preluare nelegală de documente. Sunt cazuri în care se pune la dispoziție o adresă de e-mail pentru transmitere de documente sau în cazurile investigațiilor care se realizează prin corespondență electronică, aceasta este modalitatea de comunicare. De fiecare dată urmează ca societatea emițătoare să verifice dacă există dovada legăturii dintre autoritate și adresa de e-mail pusă la dispoziție, pentru a nu exista riscul unei infracțiuni sau al unei breșe de securitate prin care s-ar dezvălui documente care conțin date cu caracter personal.

Registrul unic de control

Registrul unic de control reprezintă o condică pe care toate persoanele juridice înregistrate la Oficiul Național al Registrului Comerțului sunt obligate, prin lege, să o dețină.

Este vorba despre Legea nr. 252/2003, scopul acestui registru fiind de a păstra dovada tuturor controalelor desfășurate la contribuabil de către autoritățile specializate în domeniile: financiar-fiscal, sanitar, urbanism, calitatea în construcții, protecția consumatorului, protecția muncii, inspecția muncii, protecția împotriva incendiilor și alte domenii prevăzute de lege.

Firmele trebuie să păstreze un registru unic de control la sediul social, dar și la fiecare dintre sediile secundare care au primit autorizație sau acord de funcționare.

Registrul unic de control este tipărit de Imprimeria Națională, aflată sub autoritatea Ministerului Finanțelor Publice și nu poate fi păstrat în formă electronică, fapt care conduce așadar la păstrarea lui în formă fizică de către cineva autorizat în acest sens.

Pe Registrul unic de control se regăsesc numele și prenumele persoanelor care efectuează controlul împreună cu autoritatea de la care

provin, numărul de legitimație, detalii legate de obiectul investigației și datele de identificare ale persoanelor reprezentante ale societății și semnăturile acestora.

Pentru că acest registru urmează să fie o reală bază de date a societății în ceea ce privește persoanele participante la control, acesta se va păstra sub cheie, într-un loc sigur și nu va vor avea acces la el decât persoanele desemnate cu completarea acestuia. După fiecare prezentare și completare, se va depozita înapoi în locul de păstrare și nu se vor face copii de pe acesta pentru niciun motiv, precum nu se va scana și transmite către nicio parte terță, urmând a fi consultat doar la sediul societății.

Asigurarea implementării GDPR la punctele de acces în societate. Recepția și poarta

Accesul în companie se realizează prin puncte strategice, precum poarta de la intrarea în clădirea unde își are sediul societatea, recepția clădirii care poate fi la intrarea direct în firmă sau, dacă este vorba despre o clădire de birouri, va exista și o a doua recepție în sediul propriu-zis.

De asemenea, dacă este vorba despre firme care desfășoară activități de producție, putem regăsi un ansamblu de mai multe clădiri, fiecare cu o destinație proprie, iar accesul se face prin spații de primire multiple.

Regulile de acces în spațiile firmei se aplică angajaților societății, colaboratorilor interni sub orice titlu, care fac parte din echipa de lucru, clienților persoane fizice/reprezentanților clienților persoane juridice/potențialilor clienți persoane fizice sau reprezentanților potențialilor clienți persoane juridice/angajaților sau persoanelor fizice împuternicite sub orice titlu de partenerii contractuali ai operatorului, implicați în negocierea și derularea contractelor și oricăror alte persoane fizice, care solicită accesul într-unul din spațiile în care operatorul își desfășoară activitatea, indiferent de calitatea solicitantului, scopul și durata vizitei.

Procedura de acces în companie

Pentru implementarea unor reguli de prelucrare la accesul în societate este necesară crearea unei politici, un regulament care să stabilească în concret ce tipuri de date se prelucrează cu ocazia intrării persoanelor vizate în incintă și care sunt obligațiile operatorului față de acestea.

În afară de rolul privind respectarea drepturilor și libertăților persoanelor vizate, politica de acces trebuie să asigure verificarea și securizarea

pătrunderii în incinta societății sau în spațiile de producție, depozitare sau furnizare, după caz. Acest document va sta la baza instruirii și pregătirii personalului administrativ care este însărcinat cu verificarea accesului și colectarea de date în acest context, pentru realizarea informării adecvate a persoanelor vizate, pentru stabilirea modalității în care se va răspunde la orice tip de solicitări ale persoanelor vizate ș.a.m.d.

Accesul general trebuie făcut prin înregistrarea datelor vizitatorilor, ținând cont de principiul minimizării potrivit cu care, așa cum am mai amintit și în alte capitole, se vor colecta numai acele date necesare scopului prelucrării. Având în vedere faptul că principalul scop este acela de a preveni infracționalitatea și de a înlătura pătrunderea în incintă a unei persoane neautorizate, politica va stabili exact ce date se vor prelucra pe categorii de vizitatori, astfel încât să asigure compania că în eventualitatea producerii unui risc, este posibilă identificarea persoanei culpabile.

Modelul de registru ținut la punctele strategice de acces va fi Anexa la politică și persoanele instruite în acest sens vor ști exact care este procedura de identificare a persoanelor vizate și cum trebuie să completeze datele în el.

Dat fiind faptul că registrul de evidență al accesului va fi utilizat într-un spațiu intens tranzitat, pentru a preîntâmpina un risc semnificativ la adresa drepturilor și intereselor legitime ale persoanelor vizate, prin accesarea neautorizată a registrului, acesta va fi ținut în permanență sub supravegherea celui responsabil de controlul de acces iar în măsura în care responsabilul/înlocuitorul său nu pot asigura supravegherea directă, registrul se va depozita într-un loc securizat, inaccesibil celor neautorizați să îl consulte.



Exemplu „AȘA NU!”: Un reprezentant al unei firme de curierat vine să livreze un pachet adresat unui salariat, pe care trebuie să îl înmâneze personal. Agentul de pază îi solicită acestuia cartea de identitate și notează numele, prenumele, adresa de domiciliu și codul numeric personal pentru a se asigura că are cât mai multe date de la persoana care solicită accesul în firmă, în cazul în care se întâmplă ceva.



Exemplu „AȘA DA!”: În situația de mai sus poate fi cerut numele destinatarului pachetului, acesta poate ieși la recepție sau poartă și își poate ridica pachetul personal, fără a mai fi necesară nici măcar

identificarea persoanei curierului. Dacă acest lucru nu este posibil, datele solicitate de la curier sunt numele și prenumele și, cel mult, seria și numărul de buletin, acestea fiind date suficiente pentru situația în care va fi încălcată securitatea firmei în vreun fel.

Un alt capitol prevăzut în politica de acces trebuie să fie cu referire la durata de păstrare a datelor cu caracter personal colectate care nu trebuie să fie mai mare decât durata necesară conducerii societății să identifice făptașul, în cazul săvârșirii unui incident care produce pagube materiale, cum ar fi: furt, distrugere etc.

De regulă, orice problemă este semnalată într-un interval de timp mult mai mic decât termenul de prescripție al unei eventuale plângeri la poliție care este în general de 3 luni, de la data la care persoana vătămată a aflat despre săvârșirea faptei. Cu toate acestea, dacă nu există niciun motiv pentru care să fie necesară păstrarea registrelor cu datele vizitatorilor, acestea pot fi șterse sau distruse periodic sau se va putea stabili, în baza interesului legitim al operatorului de a promova o acțiune civilă pentru repararea unui potențial prejudiciu, un termen mai mare de 3 luni, până la 3 ani.

Destinatarii datelor colectate prin intermediul registrelor de la punctele de acces în societate nu pot fi un număr nelimitat de persoane, ci doar acelea care ar putea justifica un interes în verificarea lor.

Datele colectate cu prilejul accesului pot fi accesibile:

- membrilor conducerii societății;
- persoanei însărcinate cu paza și securitatea fiecărui spațiu sau înlocuitorului temporar al acestuia, desemnat de către cei autorizați;
- șefilor de departamente sau altui angajat/colaborator intern, însărcinat cu verificarea/confirmarea identității unui anumit vizitator, în limita atribuțiilor și responsabilităților specifice ale angajatului/colaboratorului în relațiile cu persoana vizată;
- reprezentantului DPO desemnat de operator, în vederea exercitării atribuțiilor acestuia;
- Autorității de Supraveghere și altor autorități și instituții publice competente, care solicită consultarea registrelor de acces.

Categoriile de persoane descrise mai sus sunt prevăzute cu titlu exemplificativ, nefiind o lista limitativă întrucât pot apărea și alte funcții în interiorul unei societăți care să trebuiască să verifice modalitatea în care se prelucrează datele cu caracter personal la punctele de acces, sau datele colectate însele.

Supravegherea video

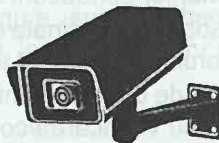
Foarte multe companii, în special cele care își au sediile în ansambluri de clădiri de birouri, au instalate camere de supraveghere fie la intrarea în edificiu, fie în interior, orientate către ușile de acces. Acestea sunt instalate în zonele publice pentru a asigura securitatea spațiilor sau ale bunurilor personalului societății și ale vizitatorilor.

În acest caz, există două tipuri diferite de abordare a înregistrărilor video, acele tipuri de sisteme de supraveghere care înregistrează magnetic imagini care sunt stocate într-un card de memorie și pot fi verificate în cazul în care intervine un incident și este necesar și sisteme de supraveghere cu monitorizare în direct de către persoane autorizate în acest sens.

Pentru ambele cazuri, dacă este implementat un astfel de sistem în zonele de acces în spațiile societății, este obligatorie poziționarea unei pictograme într-un loc vizibil pentru public pe care să fie atenționarea legată de supravegherea video. Acesta poate fi un semn care să indice o cameră și mesajul „Această zonă este supravegheată video” sau „Atenție camera de supraveghere video” etc.

Un exemplu elocvent de pictograma care ajută și la o informare corectă și completă legată de existența camerelor de supraveghere este cel întâlnit la Universitatea București:

SUPRAVEGHERE VIDEO



Operator:

UNIVERSITATEA DIN BUCUREȘTI

Activitate desfășurată în scop de
securizare / protecție a spațiilor,
bunurilor și persoanelor



Pentru informații suplimentare:

www.unibuc.ro/informare_video



Așa cum se poate observa în acest exemplu, este indicată camera de supraveghere, cine este operatorul de date cu caracter personal, scopul instalării camerei precum și link-ul către politica privind confidențialitatea și prelucrarea datelor unde persoana vizată poate să citească mai multe informații de interes.

Imaginile prelucrate de camerele de supraveghere video nu pot fi prelucrate pentru o durată mai mare de 30 de zile, așa cum prevede atât legislația europeană precum și cea națională.

Atât în contextul prelucrării datelor vizitatorilor prin completarea anumitor date în registrul ținut la poartă/recepție, precum și în cazul supravegherii video, este recomandată și o notă de informare a persoanelor vizate care să fie afișată la loc vizibil și care să conțină câteva date despre operator, temeiurile prelucrării, scopurile prelucrării, care sunt datele colectate, care sunt drepturile persoanelor vizate în legătură cu datele lor și cum le pot exercita, indicând inclusiv o adresă de e-mail sau de corespondență unde se pot adresa pentru mai multe informații.

Pentru implementarea coerentă a GDPR în ceea ce privește sistemele de supraveghere, se va ține cont de dispozițiile Regulamentului care prevăd obligativitatea operatorilor de a realiza un studiu de impact în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice. Mai multe detalii legate de efectuarea evaluărilor de impact ca măsură de protecție a persoanelor vizate vom dezvolta pe larg în capitolul privind măsurile tehnice și organizatorice.

Comitetul European pentru Protecția Datelor (E.D.P.B. – European Data Protection Board), organ cu personalitate juridică al Uniunii Europene, constituit în temeiul art. 68 din Regulamentul General privind Protecția Datelor, a adoptat pe 10 iulie Ghidul nr. 3/2019 privind prelucrarea datelor prin mijloace de supraveghere video – versiune pentru consultare publică.

Acest ghid este destinat să vină în sprijinul operatorilor de date cu caracter personal și persoanelor împuternicite ce utilizează mijloace de supraveghere video, motiv pentru care abordează, în principal, aspecte privind legalitatea prelucrării, dezvăluirea imaginilor către terți, confidențialitatea și securitatea prelucrărilor.

Potrivit ghidului, prelucrarea datelor prin supravegherea video pune o presiune suplimentară asupra individului care își poate modifica esențial comportamentul pentru a preveni detectarea a ceea ce ar putea fi perceput că o anomalie în exprimare și limitează posibilitatea mișcării anonime sau utilizării anonime de servicii.

Deși persoanele ar putea fi confortabile cu supravegherea video stabilită pentru un anumit scop de securitate, prevenire a infracționalității sau alte scopuri legale, totuși trebuie luate garanții pentru a evita orice utilizare abuzivă pentru scopuri total diferite sau neașteptate, de exemplu, scopuri de marketing, monitorizarea performanței angajaților etc., sau chiar evitarea utilizării pur și simplu incorecte din neglijență.

Cercetătorii declară că software-ul folosit pentru identificarea, recunoașterea sau analiza facială poate avea o performanță diferită în funcție de vârstă, sexul și etnia persoanei pe care o identifică. Algoritmii s-ar realiza pe baza unor demografii diferite, astfel încât tendința de recunoaștere facială amenință să consolideze prejudecățile societății și cade în responsabilitatea operatorilor să ia măsurile necesare pentru a preveni acest lucru.

Totodată, E.D.P.B. readuce prin acest ghid ideea deja dezbătută cu ocazia recomandărilor privind efectuarea de studii de impact, potrivit cu care supravegherea video nu trebuie să fie o necesitate dacă există alte mijloace pentru atingerea scopului urmărit. În caz contrar, societatea riscă o schimbare a normelor culturale care poate să conducă la acceptarea lipsei vieții private ca regulă generală.

Operatorii de date trebuie să aibă în vedere faptul că riscul potențial de utilizare necorespunzătoare a acestor date crește în raport cu dimensiunea spațiului monitorizat, precum și cu numărul de persoane care frecventează spațiul. Acest fapt este reflectat chiar de Regulamentul general privind protecția datelor în art. 35 alin. (3) lit. c), care impune efectuarea unei evaluări a impactului protecției datelor în cazul monitorizării sistematice a unei zone accesibile publicului sau a unei prelucrări la scară largă, precum și la art. 37 alin. (1) lit. b) care impune operatorilor să desemneze un responsabil cu protecția datelor, în cazul în care operațiunea de prelucrare, prin natură sa, presupune o monitorizare sistematică a persoanelor vizate.

Există și câteva excepții de la aplicarea GDPR în cazul supravegherii video, cum ar fi orice camera nefuncțională instalată, dar care nu înregistrează, deci, niciun fel de imagini, înregistrarea dintr-un unghi foarte strâns sau de la o altitudine atât de mare încât să nu poată fi distinse detalii semnificative ale persoanelor care traversează aria de supraveghere sau chiar și camerele instalate pe mașini sau alte vehicule care au ca scop orientarea pentru parcare și care bat într-un mod care nu permite identificarea persoanelor sau, în anumite cazuri, nici a plăcuțelor de înmatriculare auto.

De asemenea, ghidul arată că supravegherea video bazată pe simplul scop de „siguranță” sau informările publice de tipul „pentru siguranța dvs.” nu sunt suficient de specifice, cu excepția cazurilor în care există o obligație legală de monitorizare video, prevăzută de o lege specială.

Supravegherea video este legală și dacă este necesară pentru atingerea scopului unui interes legitim urmărit de un operator sau de o terță parte, cu excepția cazului în care interesele persoanei vizate sau drepturile și libertățile fundamentale ale acesteia nu prevalează intereselor operatorilor. Acest raport poate fi stabilit tot prin realizarea unei analize de impact în care sunt evidențiate toate datele problemei și de o parte și de cealaltă, până la stabilirea căror drepturi par a fi de natură să cântărească mai greu.

Interesele legitime urmărite de un operator sau de o terță parte pot fi legale, economice sau nemateriale. Cu toate acestea, operatorul trebuie să considere că, dacă o persoană vizată se opune supravegherii în conformitate cu art. 21 din GDPR, operatorul poate proceda la restricționarea supravegherii video a respectivului subiect, în cazul în care acesta prezintă un motiv întemeiat, bazat pe drepturile și libertățile persoanei vizate.

Având în vedere o situație reală și periculoasă, scopul de a proteja proprietatea împotriva furtului sau vandalismului poate constitui un interes legitim pentru supravegherea video. Interesul legitim trebuie să fie de existența reală și trebuie să fie prezent, nu trebuie să fie fictiv sau speculativ. O situație reală de primejdie din trecut la care s-a expus operatorul – cum ar fi daunele sau incidentele grave petrecute înainte de începerea supravegherii pot fi și acestea o dovadă puternică pentru existența unui interes legitim, precum și gradul de infracționalitate mai ridicat din cartierul sau țară respectivă. Statisticile de la autorități pot ajuta un operator să consolideze interesul sau legitim.

Totodată, situațiile de pericol iminent pot constitui un interes legitim, cum ar fi în cazul magazinelor care vând bunuri prețioase (de exemplu, bijuterii) sau în zonele bine cunoscute ca fiind tipice pentru infracțiuni de proprietate (de exemplu benzinăriile).

Urmărind un alt principiu deosebit de important instituit de GDPR, cel al minimizării datelor, E.D.P.B. menționează în ghid faptul că datele personale prelucrate trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate. A se vedea art. 5 alin. (1) lit. (c). Înainte de instalarea unui sistem de supraveghere video, operatorul trebuie să examineze întotdeauna, în mod critic, dacă această măsură este, în primul rând, potrivită pentru atingerea obiectivului dorit și, în al doilea rând, adecvată și necesară scopurilor sale. Măsurile de supraveghere video ar trebui alese numai dacă scopul

prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace care sunt mai puțin invazive pentru drepturile și libertățile fundamentale ale persoanei vizate.

Având în vedere situația în care un operator dorește să prevină infracțiunile legate de bunuri, spre exemplu, în loc să instaleze un sistem de supraveghere video, ar putea lua măsuri alternative de securitate, cum ar fi împrejmuirea proprietății, instalarea de patrulare regulate de personal de securitate sau anumite semne care să transmită mesaje clare de pericol pentru potențialii infractori.

De asemenea, apar întrebări privind necesitatea prelucrării în ceea ce privește modul în care se păstrează dovezile. În unele cazuri ar putea fi necesar să se utilizeze soluții de păstrare a materialului, iar în alte situații este posibil să nu fie necesară înregistrarea materialelor video și este mai adecvată monitorizarea în timp real. Decizia dintre cele două soluții ar trebui să se bazeze, de asemenea, pe scopul urmărit. Dacă, de exemplu, scopul supravegherii video este păstrarea dovezilor, metodele în timp real nu sunt de obicei potrivite. Uneori monitorizarea în timp real poate fi, de asemenea, mai intruzivă decât stocarea și ștergerea automată a materialelor după un interval de timp limitat. De asemenea, ar trebui să se țină cont de faptul că este posibil ca operatorul să poată folosi personalul de securitate în locul supravegherii video, care să poată reacționa și să intervină imediat.

În 2019 au fost date mai multe amenzi la nivel european, precum și în România în ceea ce privește utilizarea necorespunzătoare a sistemelor de supraveghere video, o companie de la noi din țară fiind amendată cu 5.000 de euro pentru lipsa de informare a persoanelor vizate cu privire la existența mijloacelor instalate.

În Ungaria, Comisariatul pentru protecția datelor a acordat o amendă de 15.000 de euro unei societăți (Town of Crepes) care realiza supraveghere video bazându-se pe un interes legitim nedovedit, iar Autoritatea de supraveghere din Spania a acordat o amenda de 20.000 de euro unei societăți care, deși instalase camere de supraveghere, din motive de securitate a spațiilor, a utilizat imaginile și pentru a supraveghea activitatea angajaților la locul de muncă, încălcând principiul limitării la scop.

Verificarea identității prin sisteme tehnice și imagini

Există cazuri în care, la punctele de acces în firmă există instalate sisteme tehnice care înregistrează imagini cu autoturismele care intră și ies, memorând, prin intermediul unor soft-uri, plăcuțele de înmatriculare

ale vehiculelor și uneori și imaginea per ansamblu, inclusiv cea a șoferului vehiculului. Acestea sunt asemănătoare cu cele de la poliție folosite de radar pentru a înregistra imaginea autoturismului care a depășit o anumită viteză.

Și în aceste cazuri, astfel cum am descris în subcapitolul anterior, trebuie să existe un scop foarte bine determinat pentru care se instalează un astfel de sistem, operatorul fiind obligat să justifice în mod absolut necesar utilitatea practică și faptul că același scop nu poate fi realizat printr-un alt mijloc de verificare și supraveghere al accesului, cu respectarea drepturilor persoanelor vizate.

În companiile mari, cu peste 50-100 de salariați, acolo unde controlul de acces în societate se face cu ajutorul unor cartele magnetice care au un cod specific și sunt trecute prin fața unui panou electronic, în unele situații nu este suficientă existența unei persoane cu funcția de pază, pentru că în mod real nu ar avea posibilitatea de a deosebi dacă un număr atât de mare de persoane sunt sau nu posesoarele de drept ale cartelelor. Pentru acest motiv, la punctele de acces pentru salariați există o practică privind corelarea codului de pe cartela magnetică cu imaginea salariatului respectiv care fie este afișată pe un monitor la care are acces securitatea, fie este înregistrată în sistemul operațional și se corelează automat cu seria cartelei.

În această situație, se preferă cea de-a doua opțiune, cea de înregistrare a fotografiilor cu personalul într-un sistem care să coreleze imaginea cu codul de pe cartela pentru că în acest mod se limitează accesul la imaginile cu persoanele vizate doar la câteva persoane autorizate.

Desigur că interesul legitim al operatorului pentru o astfel de prelucrare devine evident, în special în companiile unde numărul de salariați depășește 100 de persoane și angajatorul este în imposibilitate fizică de a verifica la intrare dacă persoana posesoare a cartelei este într-adevăr un angajat sau o persoană străină.

În anumite societăți încă se utilizează accesul pe bază de legitimație cu fotografie, însă la un număr mare de persoane care tranzitează zona de acces zilnic și în special în anumite intervale orare, în car este foarte dificil spre imposibil să poată fi verificate fizic toate legitimațiile.

În politica privind accesul în incintele societății urmează a fi consemnate toate măsurile tehnice și organizatorice pe care operatorul le va lua pentru a asigura o protecție adecvată persoanelor vizate supuse acestui tip de prelucrare, respectând desigur principiul limitării la scop, cel al minimizării și recurgând la ștergerea imediată a înregistrărilor, odată cu încetarea scopului prelucrării.

CNIL (Commission nationale de l'informatique et des libertés – Comisia Națională pentru Informatică și Libertăți din Franța) tratează recunoașterea facială într-un document pe care l-a publicat pe pagina sa oficială¹⁰ pornind de la principiile care stau la baza respectării drepturilor și libertăților omului și continuând cu analize detaliate legate de impactul pe care îl poate avea un astfel de sistem asupra vieții omului. Cu toate că există riscuri destul de mari, concluzionează faptul că aceste sisteme fac parte din societatea contemporană și sunt integrate tot mai des în activitatea economică, din multiple motive.

În documentul specificat se dau exemple de prelucrare a imaginii faciale a unei persoane în corelare cu un act de identitate sau pașaport în aeroporturi sau în vederea accesului la sisteme informatice sau de telefonie mobilă.

Potrivit CNIL: „recunoașterea facială se încadrează în categoria mai largă a tehnologiei biometrice. Biometria include toate procesele automatizate utilizate pentru a recunoaște un individ, cuantificându-și caracteristicile fizice, fiziologice sau comportamentale (amprentele digitale, tiparele vaselor de sânge, structura irisului etc.). GDPR definește aceste caracteristici drept „date biometrice”, deoarece permit sau confirmă identificarea unică a acelei persoane.

Ca orice proces biometric, recunoașterea facială poate îndeplini două funcții distincte:

- autentificarea unei persoane, având ca scop verificarea faptului că o persoană este cea care pretinde că este. În acest caz, sistemul va compara un șablon biometric înregistrat în prealabil (de exemplu, stocat pe un card inteligent) cu o singură față, cum ar fi cea a unei persoane care apare la un punct de control, pentru a verifica dacă acesta este una și aceeași persoană. Prin urmare, această funcționalitate se bazează pe compararea a două șabloane.
- identificarea unei persoane, care vizează găsirea unei persoane între un grup de indivizi, într-un loc, o imagine sau o bază de date. În acest caz, sistemul trebuie să efectueze un test pe fiecare față capturat pentru a genera un șablon biometric și a verifica dacă acesta se potrivește cu o persoană cunoscută sistemului. Această funcționalitate se bazează astfel pe compararea unui șablon cu o

¹⁰ <https://www.cnil.fr/en/facial-recognition-debate-living-challenges>.

bază de date de șabloane. De exemplu, poate lega o «stare civilă» (prenume, prenume) cu o față, dacă comparația se face cu o bază de date cu fotografii asociate cu un nume de familie și prenume. Poate implica, de asemenea, urmărirea unei persoane printr-o mulțime, fără a face neapărat legătura cu starea civilă a persoanei.

În ambele cazuri, tehnicile de recunoaștere facială utilizate se bazează pe o potrivire estimată între șabloane: cel comparat și cel de bază. Din acest punct de vedere, acestea sunt probabilistice. Din comparație, se deduce o probabilitate mai mare sau mai mică că persoana este într-adevăr persoana care trebuie autenticată sau identificată; dacă această probabilitate depășește un anumit prag predeterminat în sistem, sistemul va presupune că există o potrivire”.

Ce este însă și mai interesant din documentul în discuție este faptul că CNIL a identificat deja câteva modalități de utilizare a recunoașterii faciale pe care le validează ca fiind legale din perspectiva GDPR, dar și câteva exemple de prelucrări care „*nu sunt permise în societatea noastră*”, astfel cum se exprimă reprezentanții autorității.



Exemplu „AȘA DA!”: În timpul carnavalului de la Nisa, CNIL a permis testarea tehnologiei de recunoaștere facială în condiții reale pe un eșantion de voluntari, fără implicații operaționale, pentru a filtra accesul în zona carnavalului.



Exemplu „AȘA NU!”: Punerea în aplicare a sistemelor de autentificare a recunoașterii faciale a copiilor în scopul controlului accesului la școli – când obiectivele de a asigura și de a facilita intrarea în școli pot fi atinse prin mijloace la fel de eficiente, dar mult mai puțin intruzive în privința vieții private și libertăților individuale, ținând cont de protecția specială care trebuie să li se acorde copiilor.

În concluzie, abordarea pe care o au autoritățile față de acest tip de prelucrare este una obiectivă, raportată pe de-o parte la respectarea drepturilor și libertăților fundamentale ale persoanelor vizate și pe de altă parte cu înțelegere față de utilitatea acestei tehnologii. Îndemnul este de a consulta autoritatea în ceea ce privește oportunitatea de a opta pentru un astfel de sistem în defavoarea unuia mai puțin intruziv, însă mesajul este că nu se opun unei astfel de prelucrări câtă vreme operatorul va lua toate măsurile tehnice și organizatorice adecvate în scopul protecției persoanelor vizate.

Alte date prelucrate la punctele de acces

Deși în aparență, în afară de datele vizitatorilor sau ale salariaților societății, pe care îi vom trata mai pe larg ca și categorie de persoane vizate în capitolul privind implementarea GDPR în departamentul de HR, recepția pare să nu colecteze și alte categorii de date în afară de cele privind identitatea persoanelor, totuși vom reda în cele ce urmează mai multe situații care presupun date personale colectate involuntar.

În multe cazuri, secretariatul societății se identifică în același timp cu recepția, caz în care acesta este punctul în care se desface corespondența, se sortează după departamentul în care trebuie să ajungă și se dau numerele de intrare. Cu această ocazie, fiecare document pe care persoana responsabilă îl verifică pentru înregistrare poate conține date personale, în funcție de specificul său.

Fie că este vorba despre un contract cu o persoană vizată, o adresă la care se solicită răspuns, un CV pe care o persoană fizică îl lasă la recepție, fiind interesată de ocuparea unui post în respectiva societate, un proces verbal de predare primire a unor bunuri, sau orice alt document care nu emană de la un profesionist, există posibilitatea să conțină date personale.

Astfel, politica privind prelucrarea datelor prin intermediul punctelor de acces va conține cel puțin modalitatea de operare a persoanei responsabile, aceasta din urmă primind instrucțiuni foarte precise în ceea ce privește primirea, păstrarea și înmânarea documentelor către destinatarii acestora din societate.



Exemplu „AȘA NU!”: Nu se vor lăsa documente la vedere nesupravegheate, nu se vor scana și transmite pe e-mail către persoane de la care nu avem o certificare a faptului că le sunt adresate, nu sunt stocate în memoria calculatorului de lucru sau pe serverul societății într-un loc la care au acces mai multe persoane, iar păstrarea lor fizică până se distribuie destinatarilor se va face în locuri private de trafic, în dulapuri cu cheie.

Nu în ultimul rând, putem menționa și condicile sau formularele de feedback pe care unele firme le au la recepție pentru a testa experiența de client în care acesta din urmă consemnează dacă a fost satisfăcut de serviciile de care a beneficiat, dacă are solicitări speciale de la management, preferințe sau opinii pe care dorește să le împărtășească. În

această situație este necesară informarea prealabilă a persoanei vizate cu privire la faptul că datele pe care înțelege să le ofere prin respectivul formular vor fi prelucrate în vederea formulării unui răspuns sau pentru ca firma să își poată îmbunătăți serviciile pe care le oferă. Dacă va fi necesar, persoana vizată este îndrumată de asemenea să minimizeze datele pe care le oferă sau să lase un comentariu anonim, dacă are această posibilitate. Toate datele vor fi prelucrate doar în scopul în care au fost colectate.

Puncte de recepție multi-task

În funcție de specificul societății, recepția poate îndeplini și alte roluri în afară de primirea vizitatorilor și filtrarea corespondenței, cum este cazul hotelurilor sau clinicilor medicale unde se completează diferite formulare de către clienți și unde este necesar să se ia măsuri organizatorice mult mai stricte, adecvate situațiilor. Este și cazul service-urilor auto sau a magazinelor de mobilă unde clientul completează o fișă de comandă împreună cu operatorul de recepție dând date personale inclusiv adresa de domiciliu pentru livrare, date pentru garanție și retur de produs etc.

În cazul clinicilor medicale, în punctul de recepție se completează fișe de client/pacient pe care se trec date cu caracter personal precum nume, prenume, vârsta, sexul, dar și detalii legate de starea de sănătate a clientului/pacientului, alergii, intoleranțe și alte date care intră în categoria datelor speciale prevăzute de GDPR. În acest caz, rolul personalului de recepție este și de a se asigura că datele prelucrate prin intermediul său sunt gestionate într-un mod care să asigure confidențialitatea, iar politica de prelucrare a datelor nu va mai fi una redusă la activitatea de acces în sediu, ci și în legătură cu noile scopuri de prelucrare identificate. Și în ceea ce privește partea de programări la consultații este necesară o implementare coerentă a unor măsuri tehnice și organizatorice, pentru că subiecții având calitatea de persoane vizate necesită o protecție sporită a vieții lor private, riscurile la care sunt expuse fiind mult mai mari decât în cazul altor tipuri de operatori.

Dacă vorbim despre un loc de cazare, de asemenea hotelurile urmează să implementeze politici specifice care au în vedere fișele de cazare pe care unitățile nu au doar obligația să le completeze, dar și să le predea într-un exemplar secțiilor de poliție la care sunt arondate. De

asemenea, se va avea în vedere și accesul în camere, în zona de restaurant unde se servește masa, săli de conferință sau zone de relaxare la care clienții hotelului au acces.

În anul 2019, un hotel din București (World Trade Center Bucharest S.A.) a primit o amendă în cuantum de 15.000 de euro de la Autoritatea de Supraveghere națională pentru faptul că lista de hârtie tipărită utilizată pentru verificarea clienților pentru micul dejun și care conținea date personale ale 46 de clienți care au stat la hotelul World Trade Center Bucharest a fost fotografiată de persoane neautorizate din afara companiei, ceea ce a dus la dezvăluirea datelor personale ale unor clienți prin publicarea online. Operatorul a fost sancționat deoarece nu a luat măsuri pentru a se asigura că datele nu sunt dezvăluite părților neautorizate.

O altă sursă de colectare a datelor cu caracter personal cu care persoana vizată se poate întâlni încă de la intrarea în sediul unei firme este rețeaua de internet Wi-fi pe care poate alege să o utilizeze. Datoria operatorului în acest caz este să se asigure pe cât posibil de faptul că persoana vizată nu este expusă unor pericole în ceea ce privește dezvăluirea de date personale care se realizează prin conectarea la rețea.

Riscurile care pot apărea sunt de la folosirea unei rețele necriptate care poate conduce la dezvăluirea și către alți utilizatori a informațiilor de pe dispozitivul conectat, la atacuri cibernetice, analizatori de pachete de trafic, până la viruși care să colecteze informații nedorite despre persoana vizată.

Așadar este clar că, în toate situațiile expuse mai sus, precum și în altele neenumerate în prezenta carte, operatorul trebuie să aibă o atenție sporită încă de la punctul de acces în companie pentru a identifica toate canalele prin care se colectează date personale ale vizitatorilor incintei indiferent de calitatea în care sunt prezenți în incintă și să le asigure măsuri adecvate de securitate atât din punct de vedere tehnic, dar în primul rând organizatoric.

Stabilirea fluxului de date cu caracter personal în societate

După cum arătam în subcapitolul anterior, de esența implementării GDPR este stabilirea în primul rând a fluxului de date cu caracter personal în cadrul companiei.

Cum se face acest lucru?

Pornind de la organigrama societății, operatorul va răspunde cel puțin la următoarele întrebări:

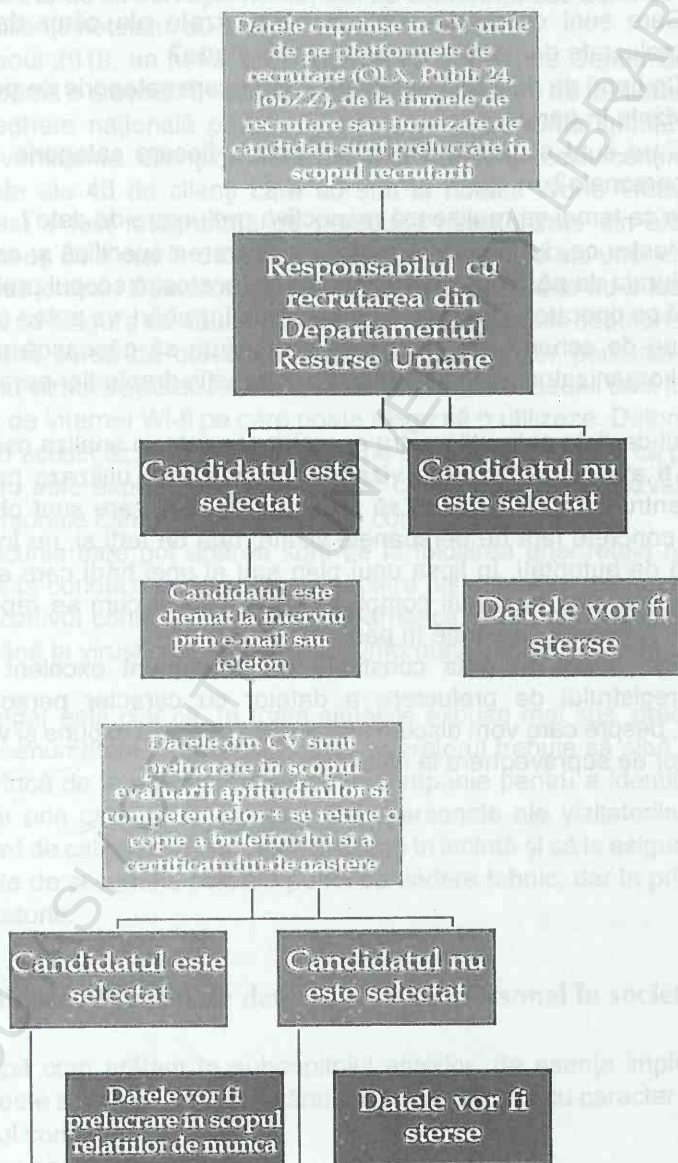
- Care sunt categoriile de persoane vizate ale căror date sunt prelucrate de fiecare departament în parte?
- Ce tipuri de date sunt prelucrate pe fiecare categorie de persoane vizate în parte?
- Care sunt scopurile prelucrării pentru fiecare categorie de date personale?
- În ce temei se realizează respectiva prelucrare de date?
- Pentru ce durată se va realiza prelucrarea specifică și care este durata de păstrare a datelor după ce încetează scopul prelucrării?

După ce operatorul va răspunde la aceste întrebări, va putea crea mai multe tipuri de scheme de lucru care să îl ajute să găsească măsurile tehnice și organizatorice adecvate pentru protecția drepturilor persoanelor vizate.

Fluxul de date este util pentru operator și pentru a analiza riscurile la care pot fi expuse persoanele vizate, cum poate să utilizeze principiile GDPR pentru ca aceste riscuri să nu se producă și care sunt obligațiile sale mai concrete față de persoanele vizate, față de terți și, nu în ultimul rând, față de autorități. În lipsa unui plan sau al unei hărți care să arate fluxul de date este mult mai complicat de identificat cum se raportează operatorul la fiecare categorie în parte.

Ulterior, fluxul de date constituie un fundament excelent pentru crearea registrului de prelucrare a datelor cu caracter personal din societate, despre care vom discuta mai pe larg pentru a expune și viziunea autorităților de supraveghere la nivel european.

Exemplu de flux de date în procesul de recrutare – Departament HR:



Din exemplul de mai sus putem observa, în primul rând, cum schema fluxului de date oferă claritate în ceea ce privește procesele de prelucrare prin care trec datele pe categorii și care sunt etapele prelucrării.

Ca document intern, fluxul de date poate fi un tabel sau o diagramă și ar putea avea în vedere identificarea categoriilor de date prelucrate, formatul în care datele sunt prelucrate, transferurile de date și locațiile în care se găsesc aceste date. Fiecare dintre aceste elemente vine cu o serie de riscuri de care compania trebuie să țină cont.

Identificarea tuturor categoriilor de date poate reprezenta o adevărată provocare pentru companie. Utilă în stabilirea fluxului de date poate fi implicarea, alături de management, a reprezentanților tuturor departamentelor companiei care pot oferi informații concrete cu privire la fiecare proces de prelucrare în care sunt implicate date personale.



● **Exemplu:** o schemă a fluxului de date pentru procesul de recrutare ar putea conține următoarele informații:

1. Datele cuprinse în CV-urile candidaților (provenite de la persoanele vizate, prin transmiterea CV-ului pe adresa de e-mail dedicată, provenite de la partenerul responsabil pentru recrutare) ajung la Responsabilul cu recrutarea din cadrul Departamentului de Resurse Umane, unde sunt păstrate în format electronic, într-un fișier securizat cu parolă.

2. Există două posibilități: candidatul nu este selectat/candidatul este selectat.

3. Candidatul nu este selectat: persoana vizată este informată telefonic, CV-ul este șters, numărul de telefon utilizat în vederea contactării persoanei în cauză este șters de pe telefonul utilizat de persoana responsabilă de informare (persoana vizată este informată telefonic inclusiv cu privire la ștergerea datelor).

4. Candidatul este selectat: persoana vizată este informată telefonic și este invitată la interviul final. Datele din CV sunt prelucrate în vederea pregătirii ofertei ferme de angajare. După acceptarea ofertei, datele persoanei vizate sunt prelucrate în vederea formalităților necesare încheierii contractului individual de muncă.

Fluxul actualizat al datelor ar trebui să stea la baza fiecărui raport emis în urma auditului periodic pe care compania îl are în vedere ca bună practică în cadrul planului de conformare.

Odată stabilit fluxul de date, se poate da eficiență principiului minimizării. Compania trebuie să identifice volumul minim de date personale

necesar în vederea scopului stabilit și să elimine datelor a căror prelucrare excedează volumului necesar prin raportare la scop.

! **Exemplu:** compania oferă servicii de închiriere trotinete electrice. Pot fi colectate în vederea furnizării serviciilor date precum nume, prenume, date card însă prelucrarea unor date legate de religie este excesivă.

! **Exemplu:** o societatea emite o factură unei persoane fizice. Poate solicita, în vederea emiterii facturii, numele, prenumele și domiciliul însă ar trebui evitat CNP-ul, din moment ce Codul Fiscal prevede faptul că acest element nu este obligatoriu pe factură.

Compania trebuie să poată demonstra faptul că în cadrul oricărui proces de prelucrare colectează și deține datele strict necesare. De asemenea, ca o bună practică, compania ar trebui să revizuiască periodic fiecare proces de prelucrare pentru a verifica dacă datele personale pe care le prelucrează sunt încă relevante și adecvate scopului stabilit la momentul colectării.

Registrul de prelucrare

Registrul activităților de prelucrare realizate de operatorii de date și de persoanele împuternicite de aceștia își are temeiul în dispozițiile art. 30 din Regulamentul 2016/679 (GDPR) și prevede obligația anumitor categorii de operatori de a ține o evidență a prelucrării datelor.

Denumit și data mapping sau cartografiere, registrul de prelucrare a datelor este o obligație doar pentru întreprinderile sau organizațiile cu peste 250 de angajați, cu excepția cazului în care prelucrarea efectuată prezintă un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii de date speciale, precum: datele care dezvăluie originea rasială sau etnică, opinii politice, confesiunea religioasă sau convingerile filozofice, apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane, datele privind sănătatea sau datele privind viața sexuală sau orientarea sexuală a unei persoane fizice.

Totodată, se menționează în GDPR obligația de a păstra o evidență a prelucrării pentru operatorii care prelucrează date cu caracter personal referitoare la condamnări penale și infracțiuni.

Nu este impusă o formă anume pe care ar trebui să o îmbrace acesta, având în vedere și diversitatea modalităților de exprimare în ceea ce privește registrele companiilor din statele membre, astfel că există o flexibilitate mare pentru responsabili cu protecția datelor.

Pentru operatorii de date care îl întocmesc având obligația legală este totuși important conținutul minim al registrului de prelucrare, după cum urmează:

a) Identificarea operatorului – numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

b) Identificarea scopurilor – scopurile prelucrării;

c) Identificarea persoanelor vizate – o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

d) Identificarea terților – categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale. Dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la art. 49 alin. (1) paragraful al doilea, documentația care dovedește existența unor garanții adecvate;

e) Identificarea duratei de prelucrare – acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date având în vedere obligații legale ale operatorului, norme interne sau acorduri cu terți;

f) Identificarea măsurilor tehnice și organizatorice – acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la art. 32 alin. (1).

Pentru persoanele împuternicite de operator, din categoria celor care au obligația legală de a ține un astfel de registru, conținutul minim prevăzut de lege se reduce la informații legate de identificarea persoanei împuternicite de operator și ale fiecărui operator în numele căruia acționează, categoriile de activități de prelucrare desfășurate în numele fiecărui operator, dacă este cazul, transferurile de date cu caracter personal către o țară terță sau a organizației internaționale respective, documentația care dovedește existența unor garanții adecvate și acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice.

Autoritatea de supraveghere din UK a publicat un exemplu de registru de prelucrare la care se pot raporta operatorii, acesta constând într-un tabel compus din coloane și linii, subsumând informațiile minime obligatorii prevăzute de GDPR.

Indiferent de modul de păstrare a evidențelor, autoritatea recomandă ca aceasta să se facă într-un mod partajat și semnificativ.

De exemplu, este posibil să existe mai multe perioade de prelucrare a datelor, acestea având legătură cu diferite categorii de date cu caracter personal. În această situație, prelucrarea datelor trebuie să conțină această diferență a tipului de date prelucrate pe respectivele perioade.

Se menționează că o simplă listă care conține o enumerare nu va fi conformă cu GDPR.

Pentru companiile care prelucrează un volum mai mare de date, au apărut soluții IT care creează nu doar registrul de prelucrare automat, ci ajută și la corelarea categoriilor de persoane vizate la temeiul de prelucrare, având posibilitatea de a controla mai ușor exercitarea drepturilor persoanelor vizate.

Modificări legislative și impactul în activitatea de prelucrare

În funcție de evoluția legislativă din fiecare stat, pot apărea situații în care se impun noi reguli de prelucrare cauzate de contextul socio-economic pe care îl traversează. Cu această ocazie, operatorii pot fi nevoiți să întocmească și alte tipuri de documente sau registre care conțin date cu caracter personal și în funcție de specificul activității trebuie adaptate la nevoile fiecăruia.

Un exemplu elocvent este criza pandemică din primăvara anului 2020, provocată de apariția virusului SARS-COV-2 în care ordinele de ministru, hotărârile de guvern sau chiar ordonanțele militare au impus restricții și reguli noi pentru operatorii de date și au creat o stare de schimbare foarte rapidă. Apariția obligațiilor privind triajul la intrările în clădiri, măsurarea temperaturii corpului uman cu dispozitive magnetice, chestionarele privind starea de sănătate a indivizilor sunt doar câteva exemple care au devenit norme impuse pentru toate categoriile de persoane și nu doar pentru cei care aveau calitatea de pacienți sau suspecți de infectare.

Drept urmare, toți operatorii au fost obligați din punct de vedere legal să se adapteze întrucât cadrul legislativ impunea o serie de prelucrări de date noi cu care nu s-au mai confruntat în trecut. Acest lucru nu se putea realiza decât printr-o cunoaștere profundă a materiei privind prelucrarea datelor cu caracter personal pentru că fiecare operator trebuia să țină cont simultan de toate regulile impuse de GDPR.

Cu toate că legea stabilește tipuri noi de prelucrare de date, regulile de colectare, stocare, arhivare și distrugere sunt tot cele prevăzute de Regulamentul European și fiecare autoritate responsabilă din statele membre are datoria să supravegheze dacă operatorii se conformează întocmai acestora. În cazul excepțional prezentat mai sus, în cadrul Plenarei Comitetului European pentru Protecția Datelor ce a avut loc în aprilie 2020, s-au adoptat o serie de documente, ghiduri ce au avut menirea să clarifice modalitatea prelucrării de date cu respectarea drepturilor fundamentale ale persoanelor vizate inclusiv în scop de cercetare științifică. În Ghidul cu numărul 3/2020 se vorbește despre faptul că toate legile adoptate în temeiul art. 9 alin. (2) lit. (i) și (j) din GDPR trebuie interpretate în funcție de principiile cuprinse în art. 5 din GDPR și ținând cont de jurisprudența CJUE. În plus, derogări și limitări în ceea ce privește protecția datelor prevăzute în GDPR trebuie să se aplice numai în măsura în care este strict necesar.

Și Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal a avut o poziție foarte puternică și a intervenit solicitând Ministerului Sănătății, Ministerului Economiei, Energiei și Mediului de Afaceri și Autorității Naționale Sanitare Veterinare și pentru Siguranța Alimentelor eliminarea art. 4 alin (1) lit. I) din Norma privind stabilirea măsurilor specifice de prevenire a răspândirii virusului SARS-CoV-2 pentru activitățile de preparare, servire și consum al produselor alimentare, băuturilor alcoolice și nealcoolice în spațiile special amenajate în exteriorul clădirilor unităților de alimentație publică, aprobată prin Ordinul nr. 966 din 29 mai 2020, respectiv Ordinul nr. 1009/2020 și Ordinul nr. 105/2020.

În concret, autoritatea nu a fost implicată în elaborarea acestor acte normative și regulile impuse pentru operatori nu respectau în același timp și drepturile persoanelor vizate prevăzute de GDPR.

Pentru operatorii de date un astfel de climat legislativ presupune o adaptare extraordinară de rapidă și o atenție sporită la modalitatea în care aleg să aplice dispozițiile legale pentru că deși apar multe obligații, totuși responsabilitatea față de cum iau deciziile rămâne o prioritate.

Exemplul de mai sus este doar unul dintre momentele în care contextul social a condus la schimbare, dar mai pot exista și altele în viitor, în special, pentru că ne îndreptăm către era digitală în care peste noapte pot apărea noi și noi tehnologii sau metode de lucru care să aducă cerințe pe zona de prelucrare de date cu caracter personal.

Arhivarea sau distrugerea documentelor care conțin date cu caracter personal

În cursul desfășurării activității zilnice, societățile gestionează și stochează diverse tipuri de documente. Importanța și sensibilitatea relativă a acestor documente se modifică conform legilor și a reglementărilor interne aplicabile.

Operatorii trebuie să respecte toate cerințele legale, de reglementare și contractuale aplicabile în ceea ce privește colectarea, stocarea, interogarea și distrugerea documentelor. În acest sens, se recomandă implementarea unui regulament la nivel intern care să traseze cadrul aplicabil tuturor persoanelor și proceselor care reprezintă sistemul de informații al organizației, inclusiv managerii, angajații, furnizorii și alte părți terțe care au acces la sistemele companiei.

Regulamentul trebuie, în primul rând, să stabilească principiile de bază care trebuie luate în considerare în ceea ce privește păstrarea și ștergerea documentelor, tipurile de documente gestionate de societate și cerințele generale aplicabile acestora. În cele din urmă, prezintă informațiile privind păstrarea, gestionarea și distrugerea documentelor.

Principii generale

Cele mai importante principii privind păstrarea și ștergerea documentelor sunt următoarele:

- Ținerea evidenței are loc în conformitate cu toate cerințele legale, de reglementare și contractuale aplicabile;
- Documentele nu trebuie păstrate mai mult decât perioada prevăzută sau necesară;
- Gestionarea efectivă a documentelor, protecția acestora din punct de vedere al integrității și disponibilității trebuie să fie în concordanță cu clasificarea de securitate a documentului;
- Documentele trebuie să fie ușor accesibile în conformitate cu cerințele mediului de afaceri și cu normele relevante de protecție a datelor;
- În cazul documentelor care conțin date cu caracter personal, cât mai curând posibil trebuie utilizate soluții pentru a împiedica identificarea automată (pseudonimizare, anonim) a persoanelor fizice asociate cu datele.

Elementele principale înregistrate de companii

a. Documente legate de afaceri

În cazul documentelor legate de afaceri, în special acordurile de cooperare, contractele, comenzile și documentele care dovedesc executarea (de exemplu, procesele verbale), pot apărea pretenții în termenul normal de prescripție în dreptul civil, prin urmare se recomandă păstrarea acestor documente timp de până la 3 ani de la executarea contractului respectiv.

Toate evidențele referitoare la subvenții primite din fonduri publice vor face obiectul unei verificări ample întrucât păstrarea documentelor referitoare la subvenții este reglementată de legea privind subvenția în cauză, de regulă posibilitatea de control s-ar putea avea loc în maxim 10 ani de la finalizarea investiției și, la acest termen se conformează și obligația de a ține evidența.

b. Registre contabile și documente necesare pentru stabilirea obligațiilor fiscale

Conform art. 25 alin. (1) din Legea contabilității nr. 82/1991, cu modificările și completările ulterioare, registrele de contabilitate obligatorii și documentele justificative care stau la baza înregistrărilor în contabilitatea financiară se păstrează în arhivă timp de 10 ani, cu începere de la data încheierii exercițiului financiar în cursul căruia au fost întocmite, cu excepția statelor de salarii, care se păstrează timp de 50 de ani.

c. Corespondență generală

Păstrarea corespondenței legate de tranzacțiile generale poate fi arhivată conform deciziei conducerii societății. Pot fi definite reguli conform cărora după o anumită perioadă de timp, administratorul de sistem sau persoana responsabilă de selectarea fișierelor electronice sau fizice va șterge sau arhiva automat aceste documente. Aceste reguli se pot schimba în funcție de departamente, volum și au în vedere orice tip de înscris, e-mail, mesaj text sau chiar audio. Deși tendința generală este de a păstra orice schimb de e-mailuri sau adrese care intră într-o societate, totuși de diligența operatorului ține să filtreze încă de la momentul primirii dacă unele dintre ele trebuie păstrate de orice fel sau pot face obiectul unei ștergeri imediate.

d. Documente legate de resursele umane

Păstrarea documentelor legate de candidați, angajați sau foști angajați se realizează aplicându-se termenele de retenție prevăzute de legislația specifică aplicabilă, cu respectarea Legii nr. 53/2003 privind Codului muncii.

În cazul recrutării, principala regulă este aceea că datele cu caracter personal ale candidaților cu care nu se încheie un contract individual de muncă după finalizarea procesului de recrutare în care aceștia s-au înscris sunt șterse. Se procedează la distrugerea documentelor fizice (CV-uri, copii ale actelor de studii ș.a.m.d.) precum și la ștergerea documentelor în format electronic permise pe e-mail.

În ceea ce îi privește pe salariații societății, dosarele lor de personal se vor păstra pentru o durată de 75 de ani, statele de salarii pentru 50 de ani, iar ordinele de deplasare și alte documente asemenea pentru 5 ani, conform legislației specifice.

e. Documente clasificate

Documentele clasificate se păstrează conform legilor speciale, Legea nr. 16/1996 a arhivelor naționale, Legea nr. 135/2007 a arhivării documentelor în forma electronică.

Cu 30 de zile înainte de începerea activităților legate de arhivarea documentelor în formă electronică, persoanele care intenționează să furnizeze servicii de arhivare electronică au obligația de a notifica autoritatea de reglementare și supraveghere specializată în domeniu cu privire la data începerii acestor activități. În consecință, apelarea la servicii externalizate în ceea ce privește arhivarea electronică va presupune o verificare prealabilă a colaboratorului ca o măsură organizatorică necesară pe care operatorul de date cu caracter personal trebuie să o adopte.

În cazul în care arhiva electronică conține sau urmează să conțină documente clasificate, administratorul arhivei electronice trebuie să îndeplinească condițiile legale privind protecția informațiilor clasificate

f. Consimțământul privind prelucrarea datelor

Contribuțiile privind gestionarea datelor sunt de regulă valabile până la revocare, cu excepția cazului în care acestea se limitează la activități specifice. În cazul revocării lor, nu va înceta doar baza legală pentru gestionarea ulterioară a datelor prelucrate în urma consimțământului (în absența unui alt temei juridic va rezulta anularea datelor cu caracter personal în cauză), dar temeiul juridic inițial legat de gestionarea ulterioară a declarației inițiale va înceta de asemenea. Totuși se recomandă păstrarea documentului care conține consimțământul și după îndeplinirea scopului consimțământului sau retragerea consimțământului, timp de 3 ani până la termenul general de prescripție în dreptul civil pe același considerent ca și în cazul contractelor, care are în vedere răspunderea civilă delictuală.

g. Datele clienților

În cadrul unei societăți furnizoare de servicii sau produse, pentru aducerea la îndeplinire a contractului, livrarea și emiterea facturilor, datele clienților sunt prelucrate în funcție de scop. Comunicarea datelor acestora se poate face prin mai multe canale, de la corespondență electronică, la încărcarea de date sau documente care le conțin în diverse platforme și până la poșta sau curier pentru suport fizic. În toate cazurile, operatorul trebuie să își pună la punct un sistem de ștergere pentru acele date colectate care nu sunt necesare, iar pentru cele păstrate în temeiul legii se vor urmări pașii explicați anterior.

Suportul de arhivare

La selectarea unui suport de stocare date pe termen lung, trebuie să se țină cont de caracteristicile fizice ale dispozitivului și de durata de utilizare a acestuia. În cazul în care legislația (sau practica) impune ca documentul să fie stocat pe suport de hârtie, trebuie luate măsuri de precauție adecvate pentru a se asigura că toate condițiile de mediu corespund tipului de hârtie utilizat. Dacă este posibil, se recomandă asigurarea unei copii de rezervă prin scanare de exemplu, cu respectarea măsurilor de securitate pe care îl impune păstrarea în format electronic.

Cu ocazia alegerii suportului de stocare și menținerii capacității de stocare, trebuie asigurat ca documentele să poată fi interogate într-un format utilizabil în termenele acceptabile.

Această interogare este deosebit de importantă având în vedere faptul că, conform GDPR, persoanele vizate au dreptul de a fi informate cu privire la datele lor personale stocate de societate. Trebuie stabilit un echilibru adecvat între costurile de stocare și viteza interogării, ținând seama în mod corespunzător de cele mai probabile circumstanțe.

Metodele de păstrare și de ștergere a documentelor trebuie să facă obiectul unei proceduri de revizuire periodică care este efectuată sub supravegherea conducerii, pentru a asigura că:

- regulile privind păstrarea și ștergerea documentelor rămân valabile,
- documentele se păstrează în conformitate cu reglementările,
- documentele sunt distruse în siguranță atunci când nu mai sunt necesare,
- respectă cerințele legale, de reglementare și contractuale,
- procesele de interogare a documentelor satisfac nevoile afacerii.

Fotografiile, filmele, microfilmele și negativele lor, rolele, bobinele sau containerele de păstrare a acestora se pot marca vizibil cu o etichetă care indică numărul și data înregistrării, precum și departamentul sau clasa de fișiere din care acestea fac parte și pentru controlul eficient al acestora se poate crea o listă de conținut. Informațiile strict secrete de importanță deosebită vor fi compartimentate fizic și înregistrate separat de celelalte informații.

Ca o regulă pentru prevenirea încălcării multiplicării prin xerocopiare sau alte mijloace tehnice pentru datele pe suport electronic, administratorul companiei va transmite tuturor angajaților indicații în funcție de categoriile de date.

Odată ce durata obligatorie de păstrare a documentelor a ajuns la sfârșitul perioadei prevăzute de regulament, acestea trebuie să fie distruse în siguranță, astfel încât să nu mai poată fi folosite. Procedura de distrugere trebuie să permită înregistrarea detaliilor de distrugere, care trebuie păstrate ca probă. În acest sens, se vor întocmi procese verbale de distrugere care vor conține cel puțin următoarele elemente:

- tipurile de materiale distruse;
- volumul și detalii care conduc la identificarea categoriei;
- modalitatea de distrugere;
- persoanele care participă la procesul de distrugere;
- data la care se realizează procedura.

Persoanele desemnate

Responsabilul cu arhivarea și distrugerea documentelor trebuie să se subordoneze nemijlocit conducerii societății, iar activitatea acestuia ar trebui monitorizată permanent și verificată prin sondaj la o anumită perioadă de timp. Dacă întâmpină dificultăți, responsabilul trebuie să se adreseze administratorului pentru suport tehnic, administrativ și financiar și pentru cazurile în care situația îl depășește poate apela inclusiv la o firmă specializată de arhivare.

Acesta ar trebui să cunoască și norme minime legale în ceea ce privește termenele de păstrare ale tuturor materialelor pe care le gestionează și atribuțiile acestuia ar trebui stabilite prin fișa postului. Instruirea lui trebuie să fie periodică și, în cazul în care există și un responsabil cu protecția datelor în cadrul firmei, sau externalizat, aceștia ar trebui să coopereze în vederea respectării prevederilor legale.

Tot acesta, se va asigura de informarea departamentului ale căror documente se arhivează sau distrug cu privire la avizarea oricăror terți care

mai pot păstra o copie de pe documente despre încetarea perioadei de stocare. În cazul în care un angajat are inițiativa arhivării sau distrugerii unui document, de asemenea se va consulta cu responsabilul desemnat.

Autoritatea franceză de supraveghere a datelor personale – CNIL a dispus amendarea companiei SERGIC cu suma de 400.000 EUR pentru protecția insuficientă a datelor personale ale utilizatorilor site-ului său web și pentru modul necorespunzător de stocare a acestor date.

Prin decizia CNIL nr. SAN – 2019-005 din 28 mai 2019, s-a reținut faptul că societatea SERGIC, specializată în dezvoltarea imobiliară, cumpărarea, vânzarea, închirierea și administrarea proprietăților, în scopul desfășurării activității sale, a creat și gestionat site-ul <http://www.sergic.com>. Prin intermediul acestui site, compania permitea clienților încărcarea și descărcarea de documente justificative necesare pentru constituirea dosarului lor și unul dintre utilizatorii care a făcut plângerea a afirmat faptul că avea acces nu doar la documentele proprii pe care le încărca pe site, dar și la cele ale altor utilizatori. CNIL a alertat compania asupra acestui incident de securitate și a încălcării în consecință a regulilor de prelucrare a datelor cu caracter personal.

Câteva zile mai târziu, s-a efectuat un control la sediul companiei. Cu această ocazie, a devenit evident că societatea era conștientă de vulnerabilitate încă din martie 2018 și că, dacă ar fi inițiat dezvoltări informatice pentru a o corecta, deficiența putea fi înlăturată complet până la data controlului.

În privința aceleiași companii s-a constatat și faptul că nu au existat proceduri de păstrare și ștergere a documentelor deși nivelul de complexitate a datelor pe care le conțineau era unul extrem de ridicat.

În concluzie, preocuparea managerului companiei față de protecția datelor cu caracter personal este ceva ce trebuie să facă parte din responsabilitățile sale curente și orice modificare organizațională sau legislativă va fi privită și din această perspectivă. Implementarea de servicii noi, deschiderea unui nou departament sau punct de lucru, încheierea de noi parteneriate și chiar schimbări ale acționariatului sunt doar câteva dintre situațiile în care o revizuire a procedurilor interne trebuie să aibă loc. Diseminarea informației în cadrul companiei se va face ori de câte ori va fi necesar pentru ca regulile de prelucrare a datelor să se aplice la toate nivelurile.

„Câștigători sunt aceia care restructurează maniera în care informația circulă în întreprinderea lor.” – Bill Gates

BUNE PRACTICI ÎN DEPARTAMENTELE JURIDIC, FINANCIAR ȘI DE RESURSE UMANE

„Pentru a avea succes, lasă de-o parte câteva din regulile vechi și învață altele noi în interesul tău și al afacerii tale”.

Bob Iger – Executive Chairman of The Walt Disney Company

Responsabilitatea aplicării corespunzătoare a Regulamentului general pentru protecția datelor revine tuturor departamentelor existente într-o societate. Organizația este precum organismul uman care, dacă are un organ slăbit, acesta va afecta și celelalte organe și, în final, disfuncționalitatea poate conduce la boală. Este necesară înțelegerea principiului potrivit cu care cooperarea în scopul evitării unei breșe de securitate e singura modalitate prin care firma poate avea un sistem sănătos de apărare a drepturilor și libertăților fundamentale privind viața privată și integritatea umană. Respectul pentru această arie de expertiză arată maturitate în business și poziționează o societate în vârful piramidei de bune practici și deontologie profesională.

GDPR este printre puținele norme legislative care vizează o companie întreagă și se aplică indiferent de specificul activității unei firme. Dacă în mod normal fiecare departament în parte urmează legi diferite și ordine sau instrucțiuni care privesc sectorul în care activează, protecția datelor este valabilă indiferent dacă ne referim la departamentul financiar-contabil, de resurse umane, de achiziții și logistică, administrativ, juridic, marketing și lista poate continua.

Explicația este aceea că în fiecare dintre aceste departamente se prelucrează date cu caracter personal pe o scară mai restrânsă sau mai largă și, deși principiile de prelucrare sunt asemănătoare, există și anumite particularități pe care operatorii trebuie să le identifice și apoi să le aplice printr-o procedura de confidențialitate a datelor implementată la nivel de companie.

Primul pas este elaborarea programului de bune practici și stabilirea concretă a măsurilor tehnice și organizatorice pe care o firmă trebuie să le adopte, următorul este crearea unor proceduri specifice pe departamente sau grupuri de salariați implicați într-o activitate comună și, în cele din urmă, asigurarea aducerii la cunoștința tuturor angajaților, colaboratorilor sau partenerilor de afaceri cu privire la responsabilitățile și modul de

gestiune al datelor cu caracter personal cu care se vor întâlni în activitatea curentă.

Într-o firmă mică unde nu există departamente sau angajați, altul decât administratorul societății sau alte câteva persoane pe partea de execuție, nu dispăre necesitatea de implementare a unei proceduri GDPR exact așa cum este necesară și existența unui regulament intern pe Codul muncii sau o condică de prezență, ci se transformă dintr-un document amplu într-un ghid mai simplu care trasează responsabilitățile fiecăruia. În ceea ce privește totuși necesitatea respectării tuturor obligațiilor față de partea de clienți și utilizatori, în cazul în care există și un website, aceasta se va realiza prin semnarea de acorduri cu fiecare furnizor de servicii în parte.

Aplicarea GDPR în departamentul juridic. Bune practici

Scopurile prelucrării

Activitatea departamentului juridic este foarte complexă, acesta deservind majoritatea angajaților societății, de la manager până la personalul administrativ, în componența sa fiind persoane care au abilități multiple de comunicare și cunoștințe ample din legislație și drept.

Departamentul juridic poate prelucra date în următoarele scopuri prevăzute nelimitativ:

- asigură negocierea, redactarea și revizuirea contractelor cu furnizorii, partenerii și clienții în activitatea societății;
- contribuie la redactarea, modificarea și revizuirea contractelor individuale de muncă și a celorlalte acte care țin de relațiile de muncă;
- menține legătura cu instituțiile statului și organele jurisdicționale, reprezentarea societății în fața instituțiilor statului și a instanțelor de judecată;
- relaționarea cu instituțiile financiar bancare, relaționarea cu instituții de colectare a debitelor/recuperarea creanțelor, precum și orice alte activități în cadrul cărora este necesar suportul juridic din partea Departamentului, ș.a.m.d.



De reținut! Orice document este transmis către angajații din departamentul juridic poate conține date cu caracter personal, motiv pentru

care trebuie să existe o atenție sporită față de acest aspect și persoana desemnată va respecta principiile prevăzute de GDPR când se va întâlni cu o astfel de situație.

Temeiurile de prelucrare la nivelul departamentului juridic

Potrivit dispozițiilor art. 6 alineat (1) literele b), c) și f) din Regulamentul 2016/679, precum și raportat la specificul activităților desfășurate la nivelul departamentului, prelucrarea de date se realizează în genere:

- pentru executarea contractelor de muncă la care persoanele vizate (salariații) sunt parte;
- pentru a face demersurile necesare îndeplinirii obiectivelor stabilite la nivelul de conducere al societății;
- pentru încheierea/executarea contractelor cu clienții și furnizorii societății în vederea îndeplinirii obligațiilor contractuale menționate în acestea;
- în vederea îndeplinirii uneia sau mai multor obligații legale (ex. prin transferul de date către autorități, instanțe, executori judecătorești);
- în vederea realizării intereselor societății, prin apelarea la instanțele de judecată în calitate de reclamant sau prin formularea apărărilor în dosarele în care societatea are calitatea de pârât;
- în scopul intereselor legitime ale societății.



● **Exemplul 1:** În cazul în care Institutul Național de Statistică transmite o solicitare de diseminare a unor date privind societatea în scopul de creștere a gradului de transparență în ceea ce privește anumite date, spre exemplu în sectorul alimentar, solicitarea va fi adresată în baza Legii nr. 226/2009 privind organizarea și funcționarea statisticii oficiale în România, motiv pentru care departamentul juridic va furniza datele solicitate în temei legal.



● **Exemplul 2:** Dacă societatea depune o cerere de chemare în judecată împotriva unui terț persoană fizică, acesta poate fi și un salariat, dar și un client, în cadrul cererii se vor dezvălui toate datele de identificare ale persoanei vizate fără a fi necesar consimțământul persoanei vizate, deoarece Codul de procedură civilă obligă reclamantul să comunice instanței toate datele precum nume, prenume, adresă de domiciliu,

ș.a.m.d., în caz contrar cererea urmând a fi anulată. Și în acest caz, temeiul prelucrării va fi cel legal.



• **Exemplul 3:** În cazul în care este necesară recuperarea unei creanțe de la un client rău platnic și acesta este persoană fizică, iar societatea decide să contacteze un avocat sau un executor judecătoresc pentru a transmite o notificare pe cale amiabilă, transmiterea datelor de identificare ale persoanei vizate către acest profesionist se va realiza în scopul interesului legitim al creditorului care se vede nevoit să furnizeze datele pentru comunicarea corectă a documentului. Avocatul mai departe va prelucra datele respective în temeiul contractului de asistență juridică pe care îl va încheia cu clientul său, în speță societatea creditoare.

În toate cazurile, angajatul departamentului juridic se va asigura înainte de orice prelucrare de date că identifică temeiul prelucrării și că poate realiza colectarea, transmiterea sau stocarea de date cu caracter personal în baza cel puțin a unuia dintre temeiurile expuse mai sus. Dacă nu identifică niciunul dintre acestea, urmează să analizeze dacă prelucrarea respectivă se va putea face doar în baza consimțământului persoanei vizate.

Responsabilitățile personalului din departament

Cu consultarea managementului societății sau șefului de departament, toți angajații trebuie să respecte cel puțin următoarele reguli de prelucrare care vor fi integrate și în fișele de post, precum și în Regulamentul intern al societății:

- Să asigure confidențialitatea datelor cu caracter personal de care iau cunoștință, să respecte dispozițiile actelor normative în privința datelor cu caracter personal, incluzând, dar fără a se limita la prevederile Regulamentului nr. 2016/679 privind protecția persoanelor fizice, în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date;
- Să nu acceseze date sau părți din datele cu caracter personal ale persoanelor vizate sau ale celorlalți angajați ai societății, în afara obligațiilor și specificului postului;
- Să nu lase nesupravegheate documente care conțin date cu caracter personal sau alte informații confidențiale și să prevină accesul persoanelor neautorizate la acestea;

- Să informeze șeful ierarhic superior sau departamentul delegat în cazul încălcării sau luării la cunoștință a unei încălcări privind protecția datelor cu caracter personal;
- Nu vor avea dreptul să ia niciun document sau suport electronic care conține acest tip de informații fără acordul prealabil al șefului de departament;
- În cazul constatării unei breșe de securitate, angajații vor informa de îndată coordonatorul departamentului, care va înainta informația către DPO, dacă există și dacă este cazul;
- Se vor asigura că revizuiesc frecvent și constant legislația în materia protecției datelor având în vedere toate circumstanțele în care se regăsesc, pentru a se asigura că modalitatea de prelucrare de date la nivelul societății se va face tot timpul în conformitate cu legislația în vigoare;
- Vor ajuta la diseminarea oricărei noutăți legislative sau procedurale către toți angajații societății care trebuie să respecte normele privind protecția datelor;
- Vor respecta normele privind arhivarea sau ștergerea datelor conform procedurilor societății.



Exemplul 1: Să presupunem că departamentul de resurse umane transmite un e-mail către un angajat al departamentului juridic pentru revizuirea unui contract de muncă al unui nou salariat. Atașată la draft-ul de contract se va regăsi și o copie de pe actul de identitate, de pe documentele care atestă nivelul de studii și cele privind starea civilă pentru asigurarea unor facilități către membrii familiei. Primul pas este identificarea faptului că toate documentele amintite mai sus nu erau necesare în vederea revizuirii contractului și juristul nu va salva pe niciun suport altceva decât contractul de muncă pentru revizuire. În continuare, va transmite un răspuns colegilor din departamentul de resurse umane prin care le va indica faptul că se încalcă principiul minimizării datelor și că le recomandă ca pe viitor să nu transmită către niciun alt departament date care nu sunt necesare.



Exemplul 2: La clinicile de chirurgie plastică și estetică private pot exista pagini create pe rețelele de socializare și, cu această ocazie, personalul să fotografieze sau să filmeze pacienții pentru a face cunoscute serviciile de calitate. Acest tip de prelucrare de date se poate face doar cu

consimțământul prealabil al clienților însă există posibilitatea ca asistentele să nu cunoască normele GDPR și cade în sarcina departamentului juridic să observe aceste detalii și să sesizeze conducerea pentru a putea implementa măsuri care să nu încalce drepturile persoanelor vizate.



De reținut! Membrii departamentului juridic sunt cei care trebuie să sesizeze ori de câte ori intervine o prelucrare nouă de date și au datoria de a informa administrația societății. Dacă există un DPO desemnat la nivelul companiei, cele două entități vor coopera în sprijinul operatorului de date.

Procedura de soluționare a cererilor și a plângerilor

Ca regulă, departamentul juridic este însărcinat cu soluționare oricăror cereri, plângeri sau sesizări pe care societatea le primește, în temeiul GDPR și nu numai.

În cazul în care se adresează o astfel de petiție care poate fi încadrată pe legislația specifică protecției datelor cu caracter personal, societatea trebuie să ofere posibilitatea persoanelor vizate să beneficieze de un răspuns.

Informațiile furnizate în temeiul art. 13 și 14 din GDPR și orice comunicare și orice măsuri luate în temeiul art. 15-22 și 34 din GDPR trebuie să fie oferite gratuit de către societate. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate să își exercite dreptul [în baza art. 12, alin. (5)] de a lua următoarele măsuri:

- să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
- să refuze să dea curs cererii.

Răspunsul la cererea depusă de persoana vizată este întocmit în formă scrisă și va cuprinde cel puțin următoarele informații:

- identitatea și datele de contact ale operatorului;
- scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- categoriile de date cu caracter personal prelucrate;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal, dacă este cazul;

- perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- sursa colectării datelor;
- drepturile persoanei vizate privind: rectificarea, ștergerea, restricționarea, opoziția și posibilitatea de a depune o plângere la A.N.S.P.D.C.P.;
- informații privind motivele respingerii cererii (dacă este cazul);
- măsurile luate în temeiul art. 15-22 și 34 din GDPR pentru soluționarea cererii (în funcție de obiectul cererii: rectificarea, ștergerea, restricționarea, portarea datelor etc.).

Răspunsul va fi expediat fie în format fizic la adresa de corespondență a persoanei vizate, menționate în cerere, fie scanat prin e-mail, la adresa de e-mail specificată de persoana vizată în cerere.

Termenul recomandat în care responsabilul din departament va furniza persoanei vizate orice informații menționate la art. 13 și 14 din GDPR și orice comunicări în temeiul art. 15-22 și 34 din GDPR este de maxim 1 lună zile. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Societatea informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.



Important! În cazul în care limba de comunicare a cererii formulate de persoana vizată este alta decât limba română, deși societatea care îndeplinește rolul de operator de date cu caracter personal este o entitate română, aceasta din urmă va îndeplini toate eforturile necesare pentru a furniza un răspuns în limba solicitantului și de a se asigura că în registrele societății va rămâne o variantă bilingvă pentru cazul în care intervine un control din partea A.N.S.P.D.C.P..

Exemplu de sancțiune acordată în România pentru neîndeplinirea obligației de a răspunde corect unei cereri de furnizare a informațiilor solicitate de o persoană vizată:

Autoritatea Națională de Supraveghere a finalizat o investigație la operatorul BNP Paribas Personal Finance SA Paris Sucursala București

(CETEM S.A.), constatând încălcarea dispozițiilor art. 12 alin. (3) din Regulamentul General privind Protecția Datelor.

Operatorul BNP Paribas Personal Finance S.A. a fost sancționat contravențional cu amendă în cuantum de 9.508 lei, echivalentul sumei de 2.000 de euro.

Investigația s-a demarat ca urmare a unor plângeri prin care se reclama faptul că operatorul nu a răspuns petentului în termenul prevăzut de art. 12 alin. (3) din Regulamentul General privind Protecția Datelor, deși acesta solicitase ștergerea anumitor date personale raportate în sistemul de evidență al Biroului de Credit.

În conformitate cu art. 12 alin. (3) din Regulamentul General privind Protecția Datelor, operatorul are obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună de la primirea cererii.

De asemenea, operatorului BNP Paribas Personal Finance SA i s-a aplicat și o măsură corectivă care a constatat în adoptarea de măsuri, la nivelul societății, cu privire la soluționarea cererilor persoanelor vizate, astfel încât să fie respectate, în toate cazurile, prevederile art. 12 din Regulamentul (UE) 2016/679.

Cum putea evita operatorul de date să fie sancționat?

Indiferent care ar fi fost obiectul cererii persoanei vizate, sancțiunea despre care discutăm mai sus nu ar fi avut loc dacă operatorul ar fi înregistrat cererea, ar fi analizat care este solicitarea punctuală și ar fi transmis un răspuns că se află în soluționare și în cel mai scurt timp se va reveni cu un răspuns. Ulterior analizei cererii, ar fi fost suficient și un răspuns negativ, dacă s-ar fi identificat un scop al prelucrării și un temei legal pentru care datele care au fost solicitate de a fi șterse trebuiau păstrate pentru o durată de timp ce preceda cererii.

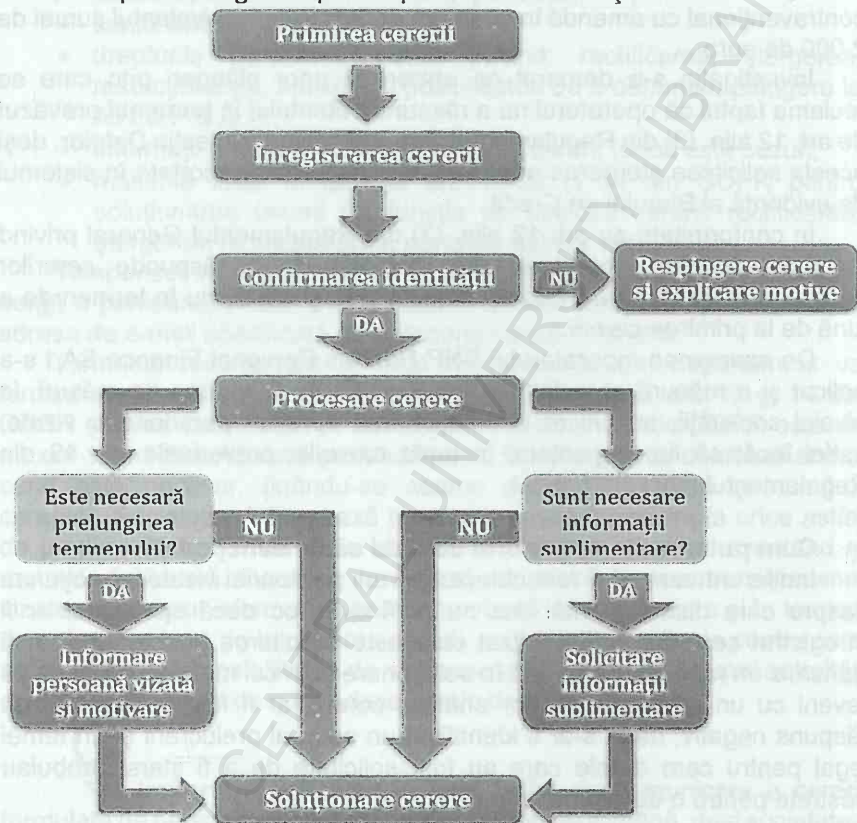
Bună practică pentru soluționarea plângerilor

Toți angajații unei societăți trebuie să aibă cunoștință de faptul că pot primi cereri sau plângeri pentru protecția datelor și pentru a putea reacționa corespunzător noi sfătuim toți operatorii să le stabilească responsabilitatea de a sesiza conducerea sau departamentul juridic.

După ce se ia la cunoștință despre existența unei astfel de situații, este necesar ca personalul abilitat să soluționeze cererea să aibă o schema clară după care să se ghideze pentru a trata sistematic toate plângerile sau cererile în același mod organizat. De mare ajutor poate fi

schema indicată mai jos care creează o claritate în procesul de răspuns, precum și o metodizare a procedurii în sine.

Exemplu de diagramă pentru procedura de soluționare a cererilor:



Procedura soluționării plângerilor împotriva răspunsului la o cerere

În exercitarea atribuțiilor sale legale, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, primește, analizează și soluționează plângeri legate de prelucrarea datelor cu caracter personal care intră sub incidența Regulamentului (UE) 2016/679.

Plângerile adresate A.N.S.P.D.C.P. trebuie formulate în scris, în limba română sau engleză, cu respectarea condițiilor prevăzute de GDPR și de

alte dispoziții legale aplicabile, precum Legea nr. 554/2004 privind contenciosul administrativ și fiscal.

Plângerile pot fi depuse la registratura generală de la sediul A.N.S.P.D.C.P. sau pot fi transmise prin poștă, inclusiv cea electronică, ori prin utilizarea formularului electronic, disponibil pe pagina de internet a A.N.S.P.D.C.P.. Plângerile primite se înregistrează în registrul general al A.N.S.P.D.C.P., primind număr și dată, și se repartizează compartimentului/compartimentelor de specialitate.

La depunerea plângerilor este obligatorie precizarea detaliată a obiectului acestora, a demersurilor întreprinse de petiționar la nivelul operatorului reclamat sau al persoanei împuternicite reclamate, după caz, a informațiilor disponibile pentru susținerea afirmațiilor, precum și anexarea de dovezi concludente, în măsura în care le deține. Fără a se aduce atingere posibilității de a se adresa cu plângere A.N.S.P.D.C.P., persoanele vizate au dreptul de a se adresa instanței competente pentru apărarea drepturilor garantate de legislația aplicabilă, care le-au fost încălcate.

Plângerile care nu au un obiect clar determinat, precum și plângerile care nu respectă condițiile prevăzute de art. 3 se resping ca fiind inadmisibile. Petiționarii sunt informați în scris cu privire la necesitatea respectării condițiilor de admitere a plângerii.

În cazul nerespectării de către A.N.S.P.D.C.P. a dispozițiilor privind procedura de soluționare a plângerilor, persoana vizată se poate adresa secției de contencios administrativ a tribunalului competent, după parcurgerea procedurii prealabile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare. Recursul se judecă de curtea de apel competentă. În toate cazurile, instanțele competente sunt cele din România.



Exemplu: O persoană vizată având calitatea de turist îi solicită agenției de la care a achiziționat un pachet de vacanță să îi transmită ce date cu caracter personal deține în legătură cu persoana sa și să șteargă orice informații se regăsesc în baza sa de date cu privire la aceasta. Agenția de turism transmite un răspuns negativ nemotivat sau nu răspunde în niciun fel solicitării. Deși motivul pentru care operatorul de date consideră că nu poate șterge datele este unul justificat de faptul că datele se regăsesc pe documente fiscale pe care firma trebuie să le păstreze pentru o perioadă de 5 ani, ștergerea fiind nelegală din perspectiva unui potențial control, faptul de a nu clarifica acest aspect față de persoana

vizată o îndreptățește pe aceasta din urmă să formuleze o plângere la A.N.S.P.D.C.P.



Atenție! Nu orice plângere formulată în fața Autorității va conduce la acordarea unei amenzi sau la o sancțiune, anumite încălcări se pot finaliza doar cu recomandări din partea A.N.S.P.D.C.P.. În cazul în care nu poate fi justificat un prejudiciu real, serios și măsurabil, cauzat de operatorul de date prin conduita sa, plângerea poate fi respinsă!



Interesant de știut! Și neglijența poate conduce la sancțiuni din partea autorităților. În dată de 6 iunie 2020, Autoritatea pentru Protecția Datelor din Spania a sancționat cu 2.000 de euro un avocat pentru încălcarea GDPR. Avocatul a citat chiriașii unei proprietăți în două ocazii, prin reutilizarea foilor de hârtie care conțineau pe verso date personale ale unor terți. Aceste date se referă la persoane fizice implicate în alte proceduri gestionate de avocatul în cauză.

Autoritatea pentru Protecția Datelor din Spania a constatat că acțiunile avocatului, care permit accesul la datele unor terți fără că aceștia să își fi dat consimțământul în acest sens, constituie o încălcare a art. 32 din GDPR – securitatea procesării.

Registrul GDPR pentru contracte

Fie că societatea încheie contracte în calitate de furnizor sau în calitate de beneficiar, în contextul GDPR este necesară analiza din perspectiva necesității inserării unei clauze privind prelucrarea datelor cu caracter personal ca urmare a semnării și a executării fiecărui contract în parte.

În cazul în care obiectul contractului impune acordarea unei atenții sporite acestui aspect, societățile pot opta pentru încheierea unui acord de prelucrare, a unei anexe la contract, sau chiar a unui contract de sine stătător prin care părțile își asumă obligații reciproce în ceea ce privește garanțiile pe care le ia fiecare în parte.

O măsură organizatorică utilă pentru companie este de a crea un registru pentru evidența contractelor încheiate și în cadrul acestuia să se specifice exact ce raport este între părțile semnatare, dacă s-a încheiat un document specific pentru prelucrarea datelor, o clauză sau nu există nicio anexă în acest sens. Acest registru poate avea multiple utilități.

Pe lângă faptul că va ajuta departamentul juridic să aibă o claritate mai mare în ceea ce privește contractele în care este angajată societatea, în cazul apariției unei breșe de securitate acest registru va fi primul care va clarifica dacă părțile aveau sau nu stabilite reguli de prelucrare de date. De asemenea, utilitatea registrului poate apărea la primirea unei cereri din partea unei persoane vizate prin care își exercită un drept.



Exemplu: În cazul în care o societate face obiectul unui *due diligence* pentru o procedură de fuziune, există anumite contracte în care se specifică foarte clar că, în cazul unei schimbări de acționariat, beneficiarul contractului trebuie să fie notificat pentru a revizui garanțiile pe care le oferă noua societate din punct de vedere al prelucrării datelor cu caracter personal. Faptul de a nu identifica o astfel de clauză și de a nu îndeplini această obligație poate conduce la preluarea unor responsabilități suplimentare în cazul unei breșe de securitate.

Exemplul de mai sus arată doar una dintre situațiile cu care se poate întâlni o firmă și indică un motiv foarte bun pentru care este recomandată implementarea unui registru de contracte. Odată cu crearea acestuia, controlul clauzelor devine mai facil și ajută juriștii să identifice mai rapid care sunt obligațiile societății în raport cu partenerii de afaceri.



Atenție! Nu este indicată utilizarea unui așa-zis draft de acord de prelucrare pe care firma în calitate de operator să îl utilizeze cu toți furnizorii sau clienții fără a fi revizuit de fiecare dată. Este greșită abordarea aceasta și pentru clauzele care sunt inserate în contracte deoarece, de la caz la caz, pot apărea particularități ale proceselor de prelucrare.

Curtea de Justiție a Uniunii Europene („CJUE”) a anunțat pe canalul său Twitter că va pronunța hotărârea în cazul Schrems II (cauza C-311/18) pe 16 iulie 2020. Această hotărâre va determina valabilitatea din Clauzele contractuale standard (Clauzele) ca mecanism de transfer în conformitate cu Regulamentul general privind protecția datelor („GDPR”). Multe companii globale, inclusiv Facebook și Microsoft, se bazează pe aceste clauze pentru transferurile internaționale de date cu caracter personal ale UE.

Avocatul general al CJUE a lansat avizul său neobligatoriu în acest caz în decembrie 2019, afirmând că, clauzele oferă o protecție suficientă pentru datele cu caracter personal. Această opinie a fost primită cu brațele deschise de întreprinderile internaționale, dar nu va fi neapărat urmată de

hotărârea CJUE. AG a susținut, de asemenea, îngrijorarea cu privire la Privacy Shield, un mecanism de transfer alternativ în cadrul GDPR, dar nu este clar dacă CJUE va face referire la Shield în hotărârea să.

În România nu există la acest moment un cadru de bune practici care să traseze clauze standard la nivel național, cu toate că, încă de la publicarea regulamentului GDPR multe organizații de antreprenori din diferite industrii au făcut eforturi deosebite pentru a putea crea un set de reguli la care să ralieze toți operatorii pentru a crea omogenitate și siguranță.

Un exemplu îl reprezintă „Asociația pentru bune practici”, fondată în anul 2018 de către noi, autoarele, în încercarea de a reuni o serie de specialiști pe protecția datelor care să traseze câteva linii generale pentru antreprenori și care să ajute la coordonarea tuturor pentru simplificarea proceselor de prelucrare în mod legal.

În acest scop, am contactat prin scrisori de intenție toate autoritățile privind protecția datelor existente la nivel european și am solicitat sprijin, sens în care am primit multe răspunsuri îmbucurătoare, acesta fiind un semn că statele sunt dispuse să coopereze între ele nu doar la nivel de sancțiuni ci și pentru a se armoniza în ceea ce privește aplicarea corectă a regulamentului.

De asemenea, alte organizații au creat coduri de bune practici care pot fi supuse avizării A.N.S.P.D.C.P., iar noi le încurajăm pe cele care încă nu au făcut-o să demareze cu toată încrederea un astfel de proces.

În Europa, la 9 aprilie 2020, Autoritatea germană de supraveghere din Baden-Wuerttemberg a publicat clauzele contractuale standard pentru persoanele împuternicite, în conformitate cu art. 28 alin. (8) din GDPR. Este prima autoritate germană de supraveghere care a făcut acest lucru și a doua din UE după ce Autoritatea daneză de supraveghere a publicat propriile clauze standard în iulie 2019. Cu toate acestea, în timp ce clauzele daneze au trecut mecanismul de consecvență GDPR în fața Comitetului european pentru protecția datelor („EDPB”), Clauzele germane nu au fost încă revizuite de către EDPB.

Atât clauzele daneze, cât și cele germane au stabilit un nivel ridicat de protecție, prin impunerea unei game largi de obligații asupra împuterniciților. Cu toate acestea, spre deosebire de clauzele daneze, clauzele germane impun obligații mai explicite decât (și, într-o oarecare măsură, depășesc ceea ce este menționat la art. 28 din GDPR). Printre alte obligații, clauzele germane impun împuternicitului să:

- facă dovada, la cererea operatorului, că personalul împuternicitului se angajează să prelucreze date cu caracter personal în conformitate cu GDPR;

- furnizeze, la cererea operatorului, un concept „complet și actualizat” de protecție și securitate a datelor pentru prelucrarea datelor;
- obțină consimțământul operatorului înainte de a autoriza personalul său să lucreze prin telemunca;
- raporteze nu numai încălcările de date către operator, ci și „tulburări” și „încălcări ale datelor suspectate” și
- aibă un registru al operațiunilor de prelucrare.

Deși împuterniciții ar putea fi deja obligați să îndeplinească unele dintre aceste obligații în cadrul GDPR, includerea lor în aceste clauze poate avea ca rezultat și răspunderea contractuală.

La 2 aprilie 2020, Autoritatea suedeză de supraveghere a indicat că respectivele clauze daneze de prelucrare pot fi utilizate și în Suedia.

Proceduri recomandate pentru conformarea cu GDPR a departamentului financiar/ contabil. Bune practici

În cadrul departamentului financiar-contabil recomandăm o procedură de lucru care să asigure protecția datelor cu caracter personal prelucrate conform cu GDPR. Scopul procedurii este de a descrie metodele de lucru și sistemele operaționale folosite pentru a garanta respectarea intimității și a dreptului la viață privată al persoanelor ale căror date cu caracter personal sunt prelucrate și stocate în sistemele companiei, ținând cont de:

- relația pre-contractuală și contractuală cu persoanele vizate, în baza căreia se realizează prelucrarea de date, în folosul acestora și pentru executarea contractului;
- tipul informațiilor pe care le colectează cu privire la persoane vizate;
- modalitățile de prelucrare a datelor cu caracter personal în cadrul companiei;
- transferul de date personale către părți terțe – prestatoare de servicii față de companie în domeniul financiar.

La nivelul Departamentului Financiar, vor fi împuternicite cu prelucrarea datelor cu caracter personal următoarele funcții: Director/manager Departament Financiar, contabil etc., cu consultarea DPO-ului.

În funcție de tipul de acces (angajat cu acces la date cu caracter personal; angajat fără acces la date, auxiliar fără acces la date, șefi de departamente) persoanele împuternicite vor lua la cunoștință de responsabilitățile lor prin fișa de post a angajatului.

Fluxul operațional al prelucrării datelor cu caracter personal

Departamentul Financiar desfășoară următoarele tipuri de activități prevăzute nelimitativ:

- întocmirea facturilor fiscale;
- gestionare și înregistrare specimene semnături aferente conturilor bancare ale societății;
- înregistrare și prelucrare date personale deschiderii de conturi de card deschise pe numele societății, având ca titular pe unul dintre angajați;
- întocmirea declarațiilor și formularelor fiscale care se vor trimite către autoritățile competente;
- transmiterea declarațiilor;
- întocmirea de adrese solicitate de diverse instituții publice sau private;
- întocmirea și transmiterea către autoritățile publice competente a Registrului electronic al zilierilor, s.a.

! ● **Exemplu:** Pentru antreprenori sau cei care desfășoară activități de free-lancer se depune o declarație unică. Declarația se completează și se depune de către persoanele fizice care realizează, individual sau într-o formă de asociere, venituri/pierderi din România sau/și din străinătate, care datorează impozit pe venit și contribuții sociale obligatorii, potrivit prevederilor Codului fiscal. Declarația se completează și se depune și de către persoanele fizice care nu realizează venituri și care optează pentru plata contribuției de asigurări sociale de sănătate.

Declarația unică pentru contribuabilii care lucrează într-o firmă prin aceste metode de asociere este prelucrată de departamentul financiar-contabil. În cadrul acestei declarații se prelucrează date precum numele, prenumele, adresa de domiciliu a persoanei vizate, CNP-ul acesteia și numărul de telefon sau adresa de e-mail.

Toate aceste date sunt prelucrate în temei legal, fiind o declarație fiscală anuală care se depune pentru stabilirea contribuțiilor fiscale ale contribuabililor.

Procedură pentru decontarea sumelor pentru concediile medicale

Cererile de recuperare a sumelor privind concedii și indemnizații de asigurări sociale de sănătate, plătite de angajatori asiguraților proprii,

suportate din bugetul FNUASS, împreună cu documentele justificative anexate, se depun la sediul CAS.

Concediile și indemnizațiile de asigurări sociale de sănătate pot fi solicitate pe baza actelor justificative, în termen de 90 de zile de la data la care beneficiarul era în drept să le solicite, conform prevederilor art. 69 din Ordinul nr. 15/1.311/2018 pentru aprobarea Normelor de aplicare a prevederilor O.U.G. nr. 158/2005 privind concediile și indemnizațiile de asigurări sociale de sănătate.

Pentru întocmirea unui dosar de decontare, cel care să conțină actele justificative se colectează date cu caracter personal cu caracter sensibil, precum adeverința de la medicul de familie care conține date privind starea de sănătate a angajatului, diagnosticul etc.

Având în vedere că sarcina decontării revine departamentului financiar-contabil, trebuie să existe o procedură care să aibă la baza confidențialitatea și responsabilitatea față de datele cu care se intră în contact.

Lucrătorii din departamentul financiar contabil vor fi instruiți cu privire la faptul că au cel puțin următoarele tipuri de obligații:

- documentele se vor păstra în mod organizat, în dulapuri cu cheie la care nu au acces alți angajați ai societății;
- nu se vor efectua copii de pe documente, dacă nu este necesar;
- nu se vor transmite informații către instituție decât după verificarea sistemelor de securitate ce permit comunicarea într-un cadru sigur;
- nu se vor dezvălui date cu caracter personal privind starea de sănătate a angajaților, decât dacă este necesar și doar către persoane autorizate în acest sens;
- după expirarea perioadei de păstrare, orice document va fi distrus etc.

Regulile de mai sus se aplică și pentru dosarele care se întocmesc pentru decontarea sumelor rezultate din incapacitatea temporară de muncă a salariaților, boli profesionale, accidente de muncă, pensii sau alte facilități acordate de autorități.



Atenție! În cazul concediilor medicale, angajații care le efectuează nu au posibilitatea de a se deplasa fizic să înmâneze angajatorului documentele de fiecare dată și trimite câte o rudă sau un alt coleg care să le aducă la birou. Dacă ne regăsim în al doilea caz, angajații ar trebui instruiți cu privire la faptul că datele care privesc starea de sănătate au caracter sensibil și că nu este indicat să procedeze în acest mod.

Societatea va face eforturi pentru a preveni această conduită, inclusiv va pune la dispoziție firma de curierat cu care lucrează pentru a împiedica o breșă de securitate.

Întocmirea documentelor pentru încasări și plăți. Facturarea

În practică se utilizează softuri pentru facturare care funcționează ca o aplicație cu mai multe câmpuri în care se completează datele necesare emiterii documentului. În funcție de aplicația folosită, unele permit includerea și a unor date precum CNP pentru identificarea persoanelor vizate atunci când este vorba de clienți persoane fizice.

Și în cazul facturilor emise pentru persoane juridice, putem întâlni câmpuri pentru introducerea reprezentantului societății, a persoanei care a întocmit factura sau a celei care primește. Din punct de vedere legal, colectarea acestor date nu este necesară și finanțistii trebuie să facă distincția când se impune completarea lor și când nu.



Important! O bună practică este utilizarea unor aplicații care nu sunt standard și care permit emiterea facturilor fiscale fără CNP.

Potrivit Codului Fiscal, CNP-ul nu este un element obligatoriu necesar a fi înscris în cuprinsul facturii, fiind oportun în contextul noii reglementări europene ca datele cu caracter personal înscrise pe facturi să se limiteze la nume, prenume și eventual adresa de domiciliu completă (în plus, așa cum se menționează în OMFP nr. 2264/2016 completarea CNP/NIF este obligatorie în situația în care persoana impozabilă îl colectează de la persoană fizică din facturi, contracte (de prestări servicii, de furnizare utilități, vânzări de bunuri mobile și imobile etc.); în lipsa acestuia, se vor declara numele, prenumele și adresa persoanei fizice.).



Atenție! Și modalitatea de transmitere a facturii este foarte importantă. Trebuie aleasă o cale care să nu permită încălcarea drepturilor vizate prin dezvăluirea de informații către persoane neautorizate.



Exemplu de încălcare 1: În 2018 A.N.S.P.D.C.P. anunță că operatorul de telefonie fixă și mobilă Telekom România Mobile Communications S.A. a fost amendat cu o suma modică de 9.544,40 lei,

echivalentul sumei de 2.000 de euro pentru încălcarea art. 5 alin. (1) lit. (d) din Regulamentul (UE) 679/2016.

În ce au constat neregulile?

Sancțiunile au fost aplicate ca urmare a unor plângeri prin care se menționează faptul că reclamantul primește la adresa sa de domiciliu facturi adresate unei alte persoane, client al operatorului, precum și faptul că a semnalat operatorului această situație, dar nu a primit răspuns.

Pe lângă încălcarea în sine de a fi transmis din eroare factura unui client către un alt client, observăm și încălcarea obligației de a formula un răspuns la plângerea persoanei vizate, atitudine pe care o tratăm separat în capitolul destinat procedurii soluționării plângerilor.



● **Exemplu de încălcare 2:** La data de 27.06.2019, Autoritatea Națională de Supraveghere a finalizat o investigație la operatorul UNICREDIT BANK S.A. și a constatat că acesta a încălcat prevederile art. 25 alin. (1) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

Operatorul a fost sancționat contravențional cu amendă în cuantum de 613.912 lei, echivalentul în euro al sumei de 130.000 de euro.

Sancțiunea a fost aplicată UNICREDIT BANK S.A. ca urmare a neaplicării măsurilor tehnice și organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele RGPD și a proteja drepturile persoanelor vizate.

Aceasta a condus la dezvăluirea în documentele ce conțin detaliile tranzacțiilor și care sunt puse online la dispoziția clienților beneficiari ai plăților, a datelor privind CNP-ul și adresa plătitorului (pentru situațiile în care plătitorul efectua tranzacția dintr-un cont deschis la o altă instituție de credit – tranzacții externe și depuneri la casierie), respectiv a datelor privind adresa plătitorului (pentru situațiile în care plătitorul efectua tranzacția dintr-un cont deschis la UNICREDIT BANK SA – tranzacții interne), pentru un număr de 337.042 persoane vizate, în perioada 25 mai 2018 – 10.12.2018.

Sanctiunea a fost aplicată ca urmare a unei sesizări a Autorității Naționale de Supraveghere din data de 22.11.2018 prin care se semnala faptul că, datele privind CNP-ul și adresa persoanelor care efectuau plăți la UNICREDIT BANK S.A., prin intermediul tranzacțiilor online, erau dezvăluite către beneficiarul tranzacției, prin formularele de extras de cont/detalii.

Potrivit art. 5 alin. (1) lit. c) din RGPD („Principii legate de prelucrarea datelor cu caracter personal”), operatorul avea obligația de a prelucra date limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate datele.

Obligația legală de păstrare a facturilor fiscale care pot conține ocazional date cu caracter personal este de 10 ani, conform Ordinului Ministerului Finanțelor Publice nr. 2634/2015 privind documentele financiar contabile în vederea punerii la dispoziția organelor de control documente privind corecta înregistrare în evidențele contabile a operațiunilor.

Procedura de prelucrare a datelor cu caracter personal în cadrul gestionării procesului de recuperare a creanțelor

Departamentul financiar pune la dispoziția departamentului juridic date cu caracter personal ai debitorilor persoane fizice care au înregistrat întârzieri în plata creanțelor către firmă. Astfel, departamentul juridic îndeplinește pe mai departe procedurile legale necesare în vederea îndeplinirii acestor creanțe.

Departamentul financiar va prelucra următoarele tipuri de date cu caracter personal:

- Numele, prenumele și adresa debitorului persoană fizică;
- Codul numeric personal al debitorului;
- Contul bancar al debitorului.

În condițiile legii, au dreptul să acceseze datele cu caracter personal și profesional înscrise în contracte și pe facturi următoarele persoane:

- Debitorului persoană fizică;
- Departamentul juridic sau un avocat;
- Instanțele judecătorești competente;
- Executorul judecătoresc competent;
- Orice alte instituții către care operatorul are obligația de a furniza date cu caracter personal conform legislației în vigoare;

- Personalul din Managementul superior al societății;
- Personalul care lucrează în bancă pentru decontarea unor instrumente de plată etc.

Niciun angajat, indiferent de nivelul de autoritate/control deținut în cadrul companiei, nu va dezvălui sau transmite date cu caracter personal de care ia cunoștință în exercitarea funcției în afara cadrului organizațional intern și nu va utiliza informații private pe care le deține cu privire la colegii săi în alte scopuri decât cele legale și necesare desfășurării activității sale.

Accesul în birourile/sediile unde se prelucrează date cu caracter personal este restricționat, având acces doar persoanele din cadrul departamentului financiar care au trecut în fișa postului astfel de responsabilități. Căile de acces sunt monitorizate, fiecare angajat depune diligența să se asigure că încăperea/biroul unde se prelucrează date să nu rămână niciodată nesupravegheat. În situația în care toți membrii biroului lipsesc, ușile și ferestrele trebuie verificate și închise.

Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.



Important! În ceea ce privește anumite contracte garantate cu instrumente de plată, putem întâlni pe biletele la ordin numele și prenumele avalistului persoană fizică, acesta fiind de cele mai multe ori administratorul societății. Urmărirea silită a avalistului nu este permisă decât în cazul unei proceduri de executare silită desfășurată în condițiile legii.

Faptul de a notifica administratorul pe datele sale personale în vederea recuperării unei sume avalizate printr-un bilet la ordin este nepermisă și reprezintă printre altele și o încălcare a dreptului la viață privată a acestuia.



Exemplu „AȘA NU!”: Dacă o firmă are de colectat debite de la clienți persoane fizice și dorește să le transmită notificări de plată, poate utiliza adresa de e-mail pusă la dispoziție de către client sau adresa de domiciliu a acestuia, însă nu este legală transmiterea unei notificări care să conțină date cu caracter personal la locul său de muncă, în special către adrese de fax sau e-mail la care au acces alte persoane decât aceasta.

Tipurile de date colectate în departamentul financiar-contabil. Particularități și exemple

Date prelucrate de departamentul financiar contabil

În departamentul financiar-contabil se prelucrează în general următoarele tipuri de date prevăzute nelimitativ:

- numele și prenumele, numele și prenumele membrilor de familie, funcția deținută salariați;
- date referitoare la condițiile de muncă;
- semnătura;
- starea de sănătate;
- situația economică și financiară;
- date bancare;
- numărul asigurării sociale/asigurării de sănătate;
- adresă de domiciliu;
- telefon/fax, e-mail;
- codul numeric personal, codul numeric personal al membrilor de familie;
- datele de identificare ale clienților persoane fizice sau reprezentanților persoanelor juridice etc.

Înmânarea fluturașilor de salariu

Fluturașul de salariu este un act prin care angajatorul își informează salariații despre veniturile și contribuțiile sale în momentul plății pe care o face pentru muncă pe care aceștia au prestat-o și nu reprezintă un document fiscal.

Tocmai pentru că nu este o obligație fiscală a angajatorului, acesta poate să îmbrace mai multe forme și poate conține mai multe sau mai puține date cu caracter personal, în funcție de ceea ce alege angajatorul să scrie. Dat fiind acest fapt, recomandarea este să fie utilizat doar dacă este necesar, eventual la cererea salariatului și să fie comunicat într-una din următoarele modalități:

- fizic – pe suport de hârtie, înmânat personal, în plic sigilat;
- prin e-mail;
- printr-un program care gestionează documentele companiei.

O buna practică este aceea de a reduce la minimum datele cu caracter personal de pe fluturașul de salariu prin eliminarea oricăror date care nu

sunt necesare, putând fi utilizată chiar și pseudonimizarea numelui și a prenumelui prin inițiale sau un cod pe care i-l alocă salariatului.

În Finlanda, spre exemplu, angajatorul este obligat prin lege să trimită angajaților fluturașul de salariu (payslip). Astfel, recomandările ar fi ca trimiterea acestora să se facă printr-o platformă securizată în care fiecare angajat să aibă acces pe baza de parolă persoană, prin e-mail, la adresa aleasă de angajat și numai cu acordul prealabil al angajatului, ori prin poștă normală. O altă măsură recomandată pentru respectarea (în Marea Britanie) a GDPR ar fi ștergerea acestor fluturași de salariu după ce au fost trimiși (UK Bureau).



Exemplu „AȘA NU!”: O încălcare a GDPR este înmânarea fluturașilor de salariu prin lăsarea acestora pe birou chiar dacă persoană nu se află la birou.



Exemplu „AȘA DA!”: Dacă procedura utilizată în cadrul companiei este de a înmâna fluturașul de salariu personal și acesta nu se află la birou, personalul departamentului financiar îl va păstra până când va avea posibilitatea să i-l ofere nemijlocit.

Orice dezvăluire a datelor cu caracter personal conținute pe fluturașul de salariu, neautorizată în prealabil de persoana vizată, constituie o breșă de securitate și va fi tratată ca atare.

Acordarea tichetelor de masă

Conform Legii nr. 165/2018 biletele de valoare care pot fi acordate sunt: tichete de masă, tichete cadou, tichete de creșă, tichete culturale și vouchere de vacanță.

Tot potrivit aceleiași legi, în ceea ce privește tichetele de masă acordate de angajator, sunt valabile și pot fi supuse decontării doar dacă au înscris numărul sub care a fost înscris de către unitatea emitentă și cuprinde cel puțin următoarele mențiuni:

- a) numele și adresa emitentului;
- b) valoarea nominală a tichetului de masă;
- c) perioada de valabilitate a utilizării tichetului de masă;
- d) spațiu pentru înscrisul numelui, prenumelui și codului numeric personal ale salariatului care este în drept să utilizeze tichetul de masă;

e) interdicția de a fi utilizat pentru achiziționarea de țigări sau de produse alcoolice;

f) spațiu destinat înscrierii datei și aplicării ștampilei unității la care tichetul de masă a fost utilizat.

Dat fiind că este necesară înscrierea datelor prevăzute mai sus la punctul d), care sunt eminamente date cu caracter personal, departamentul financiar are obligația de a se asigura de faptul că acestea sunt înmânate angajaților într-o manieră care nu permite dezvăluirea lor către terțe persoane neautorizate și se va proceda ca și în cazul fluturașilor de salariu.



● **Exemplu de prelucrare a datelor prin tichete cadou:** În campaniile de stimulare a vânzărilor, o firmă poate acorda tichete cadou clienților săi, pe lângă alte bunuri sau produse pentru testare. Pentru bunurile acordate gratuit în cadrul campaniei de stimulare a vânzărilor, se întocmește un aviz de însoțire în care se precizează următoarele aspecte:

- numele și prenumele clientului, inclusiv datele de identificare ale acestuia;
- cantitatea și valoarea tichetului acordat;
- mențiunea „Nu se facturează! Campanie de stimulare a vânzărilor în conformitate cu Regulamentul nr. .../dată...”

Prin acest document justificativ se confirmă predarea tichetului cadou către client și se efectuează descărcarea de gestiune a tichetului și înregistrarea cheltuielilor de stimulare a vânzărilor.

Decontarea cheltuielilor pentru deplasări

În cazul deplasărilor efectuate de salariații unei societăți în altă localitate decât cea în care își desfășoară în mod curent activitatea, pentru decontarea cheltuielilor efectuate cu drumul, cazarea, masa și altele asemenea, se prezintă o serie de documente care fac dovada. Procedura operațională privind decontarea cheltuielilor de deplasare/delegare în altă localitate, în interesul serviciului, se aplică tuturor persoanelor care sunt implicate, prin atribuțiile stabilite în fișa de post, în activitatea privind decontarea cheltuielilor de deplasare.

Ordinul de deplasare se completează de către titularul său cu următoarele date cu caracter personal:

- numele și prenumele,
- funcția și departamentul în care lucrează,

- localitatea în care se va deplasa și în ce scop,
- data deplasării,
- alte informații care nu reprezintă date cu caracter personal.

În ceea ce privește datele obișnuite privind identificarea persoanei salariatului, se vor aplica aceleași reguli de prelucrare amintite mai sus, însă apare o particularitate, aceea a locației unde se deplasează angajatul cu indicarea localității și a locului de cazare. Documentele privind cazarea se atașează ordinului de deplasare și se ridică în practică întrebarea dacă faptul de a se dezvălui față de un terț locul unde doarme propriu-zis persoana vizată pe durata deplasării reprezintă sau nu o încălcare a vieții private, de vreme ce nu este locuința sa, ci un amplasament pus la dispoziție de angajator pentru odihnă în timpul deplasării.

Mai mult decât atât, atunci când rezervarea hotelului se realizează direct de la sediul angajatorului, unitatea de cazare va solicita datele de identificare ale acestuia pentru a efectua rezervarea și la momentul preluării camerei ce cere și o copie de pe cartea de identitate.

Răspuns: În cazul dezvăluirii locației de cazare față de persoane neautorizate, ne aflăm în prezența unei breșe de securitate, deoarece există posibilitatea de a i se încălca viața privată a salariatului chiar dacă deplasarea și implicit cazarea sunt efectuate în interes de serviciu.

Pentru a încadra incidentul ca fiind o încălcare a drepturilor fundamentale, trebuie să analizăm dacă intimitatea și securitatea persoanei vizate sunt puse în pericol, fapt ce este afirmativ. Persoanele vizate sunt singurele care decid dacă își dezvăluie locația atunci când nu sunt la serviciu și tot ele decid către ce persoane. Singura dezvăluire legală a datelor privind unitatea de cazare se poate realiza către managementul societății, departamentul de HR sau alte departamente administrative care pot fi implicate în acest proces. Dacă există mai multe departamente între care circulă documentele de decontare, salariatul trebuie să fie informat cu privire la fluxul pe care îl vor parcurge datele sale, în ce scop și pentru ce durată vor fi păstrate.

Excepție! De la regula de mai sus există și o excepție, dacă salariatul și-a făcut publică locația din proprie inițiativă, spre exemplu, pe o rețea de socializare, având contul public și cu acces din partea oricui.



Exemplu „AȘA NU!”: Transmiterea cărții de identitate a salariatului către unitatea de cazare sau către organizatorul unui eveniment/conferință la care acesta va participa fără a fi necesar.

Prelucrarea datelor din cartea de identitate este excesivă și încalcă principiul minimizării datelor cu caracter personal, conform GDPR.



Atenție! Departamentul financiar, în exercitarea atribuțiilor sale, nu va ține niciun fel de registre sau evidențe care nu sunt necesare, cum ar fi liste cu salariații care sunt în concediu medical, liste cu salariații care au copii minori pentru eventualitatea în care se organizează un eveniment cu participarea acestora sau copii de pe documentele care conțin date personale ale salariaților și nu au un scop precis. De asemenea, nu se vor printa și îndosaria facturi sau chitanțe care conțin date cu caracter personal ale clienților decât în cazul unui control, pentru a face dovada în fața autorităților competente.

Proceduri recomandate pentru conformarea cu GDPR a departamentului de HR. Bune practici

Departamentul de resurse umane este cel în care se prelucrează cel mai mare volum de date personale și cu cele mai complexe procese de prelucrare.

Fie că ne aflăm în etapa de recrutare, în cursul derulării relațiilor de muncă sau chiar și după încetarea unui contract, se prelucrează constant date ale salariaților, membrilor familiilor acestora sau ale colaboratorilor cu care interacționează societatea.

Managementul resurselor umane a cunoscut o schimbare impresionantă în ultimele decenii. Dacă în urmă cu 20 de ani rolul oamenilor de resurse umane era mai degrabă unul administrativ, constând în recrutarea forței de muncă, calculul salariilor și pregătirea dosarelor angajaților, peisajul și rolul HR-ului în prezent este unul strategic.

Rolul HR-ului actual este să dezvolte un plan cu inițiative specifice, să dezvolte cultura companiei și să o facă cunoscută în interiorul și în exteriorul ei, precum și să asigure acele competențe necesare ca organizația să-și atingă obiectivele de business.

Toate acestea, nu se pot desfășura în mod corespunzător fără prelucrarea de date personale, în ultimii ani din ce în ce mai multe, în special pentru că ne aflăm în era digitalizării care include multă vizibilitate în mediile on-line, cu implicarea angajaților în tot ce înseamnă promovarea companiei față de clienți.

Tipuri de activități desfășurate de departamentul resurse umane

Departamentul resurse umane desfășoară următoarele tipuri de activități, prevăzute nelimitativ:

- primirea CV-urilor;
- desfășurarea interviurilor;
- întocmirea dosarului de personal;
- înregistrarea contractelor de muncă, modificarea contractelor de muncă (ambele acțiuni cu raportare în REVISAL);
- monitorizarea prezenței angajaților;
- întocmirea ștatelor de plată;
- transmiterea declarațiilor;
- întocmirea de adeverințe destinate unor instituții publice sau private;
- eliberarea de diplome/certificate de calificare;
- organizarea de teambuilding-uri sau alte activități recreative;
- organizarea cursurilor de formare profesională;
- participă la redactarea și respectarea regulamentului intern și a contractului colectiv de muncă;
- participă la evaluarea profesională a salariaților;
- participă la cercetările disciplinare ale angajaților societății;
- redactează scrisori de recomandare pentru foști salariați etc.

Prezentul capitol își propune să trateze o parte din procesele de prelucrare care se desfășoară la nivelul departamentului de HR (Human Resources) cu exemple de bune practici și greșeli pe care le pot face membrii departamentului și care pot conduce la încălcări care mai departe riscă sancțiuni din partea A.N.S.P.D.C.P.

Tipuri de date cu caracter personal prelucrate de departamentul de resurse umane

Departamentul de resurse umane prelucrează următoarele tipuri de date cu caracter personal, prevăzute nelimitativ:

- numele și prenumele salariaților, numele și prenumele membrilor de familie,
- locuri de muncă anterioare,
- formare profesională – diplome – studii;
- data și locul nașterii, sexul;
- religia;

- situația familială, date din actele de stare civilă, cetățenia;
- situația militară;
- semnătura;
- situația economică și financiară;
- date bancare;
- date din permisul de conducere;
- date din dosarului de pensie sau de asigurării sociale/asigurării de sănătate;
- adresă de domiciliu, telefon/fax, e-mail;
- codul numeric personal;
- date privind sancțiuni disciplinare, litigii;
- date privind starea de sănătate;
- date conținute în cazierul judiciar;
- imaginea etc.

Prelucrarea de date în faza de recrutare. Particularități

Datele cu caracter personal pot fi colectate atât în faza de recrutare prin transmiterea CV-urilor online sau înmânarea acestora la un târg de joburi sau evenimente de networking, cât și în faza de administrare resurse umane (în principal la întocmirea dosarului de personal). De asemenea, datele cu caracter personal pot fi colectate și în perioada calculului salarial (concediile medicale, concedii de odihna, ștatelor de plată).

Când este necesar consimțământul persoanei vizate?

- Căduatții pentru un post care aplică prin intermediul mijloacelor online vor primi pe e-mail o atenționare cu privire la prelucrarea datelor lor cu caracter personal, care va conține cel puțin scopul prelucrării datelor personale, temeiul prelucrării, drepturile de care beneficiază în baza Regulamentului 2016/679 și perioada de timp pentru care datele lor vor fi păstrate la care va fi atașat formularul privind, aceasta fiind o informare.

- Persoanele care aplică în mod fizic la procesul de recrutare prin depunerea CV-ului la registratura societății, la târguri de recrutare etc. vor fi rugate să semneze pe loc formularul privind luarea la cunoștință a tuturor detaliilor legate de scop, durata de păstrare ș.a.m.d.



Atenție! Persoanele care participă la procesul de recrutare pentru un post ar trebui să fie informate cu privire la durata procesului de recrutare, pentru a avea o predictibilitate în ceea ce privește utilizarea

datelor lor. Nu este permisă păstrarea unor CV-uri la finalizarea procesului de recrutare pentru eventualitatea contactării candidatului în viitor, să zicem în cazul în care mai apare un post similar.

Dacă angajatorul are o astfel de procedură de selecție cu păstrarea CV-urilor într-o bază de date care poate fi utilizată și ulterior, va fi necesar consimțământul expres al persoanei vizate care poate fi luat fie anterior, prin transmiterea unui consimțământ expres în acest sens, fie odată cu răspunsul de respingere.

- Persoanele angajate vor fi informate în momentul angajării cu privire la prelucrarea datelor cu caracter personal și vor consimți atât prin semnarea contractului de muncă, cât și a unei notificări informative.

De fiecare dată când urmează ca datele personale ale noului angajat sau ale candidatului să fie prelucrate în alte scopuri decât cele expres menționate în cadrul procesului de informare inițială, acesta trebuie să fie informat în mod complet și corect despre prelucrarea ulterioară.

Conținutul minim al notei informative la angajare:

- tipurile de date prelucrate;
- scopurile prelucrării;
- temeiurile în baza cărora se realizează prelucrarea de date;
- terțe părți către care se vor transmite datele lor cu caracter personal, pe categorii (Ex. Firma de payroll, firmă externalizată de contabilitate, societate de avocatură etc.);
- durata de păstrare a datelor cu caracter personal;
- măsurile tehnice și organizatorice pe care le ia angajatorul în calitate de operator de date cu caracter personal care asigură protecția lor;
- drepturile lor în calitate de persoane vizate conform GDPR;
- datele autorității de supraveghere pentru eventualitatea formulării unei plângeri.

Despre prelucrarea datelor din cazierul judiciar

Prelucrarea datelor din cazierul judiciar se poate face în temeiul art. 6 alin. (1) GDPR privind legalitatea prelucrării:

„c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate,

care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil”.

Model de cazier judiciar:

MINISTERUL ADMINISTRAȚIEI ȘI INTERNELOR
INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE
Direcția Cazier Judiciar, Statistică și Evidențe Operative

Seria N Nr. 0725072

- Cazier Judiciar -

caziera personal nr. 64

Certificat de cazier judiciar

Nr. XXXXXXXX din XXXXXXXX

Numele XXXXXXXXXX	Prenumele XXXXXXXXXX
Data nașterii XXXXXXXXXX	C.N.P. -----
Locul nașterii -----	XXXXXXXXXX
Ultimul domiciliu -----	XXXXXXXXXX

Solicitantul nu este înscris în cazierul judiciar.

S-a eliberat prezentul certificat spre a-i servi la: XXXXXXXX

ȘEFUL CAZIERULUI JUDICIAR.

LS
PA

CONFIDENTIAL

După cum se poate observa în imaginea de mai sus, cazierul judiciar este un document care conține și CNP-ul, motiv pentru care se impune consimțământul persoanei vizate, dacă angajatorul dorește să colecteze aceste date, ele nefiind necesare în mod normal la dosarul de salariat.

Există anumite profesii în care prelucrarea datelor din cazierul judiciar este necesară pentru verificarea reputației viitorului angajat, cum ar fi: medicii, farmaciștii, consilierii juridici, sau profesii ale căror atribuții presupun lipsa antecedentelor penale: gestionar, casier, trezorier, șef restaurant, lucrător bancar ș.a.



Recomandare: verificarea reputației prin consultarea certificatului de cazier judiciar și returnarea acestuia persoanei vizate. Rațiunea acestui mod de operare este cu atât mai întemeiată cu cât valabilitatea cazierului judiciar este de maximum 6 luni și păstrarea acestuia la dosarul

salariatului nu are oricum nicio relevanță, dat fiind faptul că un angajat poate săvârși între timp o infracțiune.

În caz contrar, avem de-a face cu:

- Încălcarea principiului reducerii la minimum a datelor;
- Discriminare indirectă – fapt care încalcă dispozițiile referitoare la egalitatea în activitatea economică în materie de angajare, încălcare care conduce la aplicarea sancțiunii contravenționale prevăzute la art. 26 din Ordonanța nr. 137/2000 privind prevenirea și sancționarea tuturor formelor de discriminare.

Legitimațiile de serviciu, pontajele și permisele de parcare

Legitimația

La încadrarea unui salariat, în special în societățile cu un număr mare de angajați, devine o necesitate asigurarea unei legitimații din partea societății. Modelul de legitimație este stabilit de conducere, cu participarea departamentului de HR sau administrativ și poate îmbrăca diverse forme și funcționalități.

Recomandarea este de a minimiza datele pe care le conține, astfel încât să protejeze, pe cât posibil, datele cu caracter personal ale angajaților și totuși să deservească scopului. Legitimația poate fi utilizată doar în scopul de a verifica apartenența unui membru al echipei la intrarea în firmă sau poate fi utilizată și în scop de card de acces digital, potrivit unui sistem electronic.

Au fost introduse în uz la acest moment sisteme de pontaj electronic care pot gestiona până la 20.000 de angajați ce pot fi împărțiți în zeci și sute de departamente. Unele dintre ele au recunoaștere facială a salariatului, altele permit un cod care transmite accesul în întreprindere ca simple cartele magnetice, iar în cazul în care intrarea se poate face fără utilizarea unui card electronic se pot implementa legitimații simple care conțin informațiile de bază pentru identificarea salariatului.

În toate cazurile, preocuparea operatorului de date este de a crea un sistem bazat pe numere și serii care să reducă la zero necesitatea de a folosi datele personale ale persoanelor vizate. La departamentul de HR ar trebui să existe o listă a angajaților care să atribuie fiecăruia un cod format din cifre și care să nu permită identificarea persoanei decât de către un număr restrâns de oameni care gestionează accesul în firmă sau pontajele.



Exemple „AȘA NU!”:

1. Modelul de legitimație care conține fotografia salariatului, numele și prenumele, funcția pe care o deține și departamentul din care face parte.
2. Un alt exemplu negativ este utilizarea cardurilor de acces în întreprinderi care au la intrare un monitor pe care se proiectează imaginea persoanei vizate care utilizează cardul.

În vederea respectării vieții private a angajaților și pentru prevenirea încălcării drepturilor acestora, angajatorii trebuie să manifeste o preocupare sporită față de datele personale salariaților. În afara instituțiilor publice cu funcții care au reglementate prin lege modelul de legitimație și care este necesară în cazul efectuării unui control, în mediul privat există o flexibilitate sporită în ceea ce privește conținutul acestora. Pentru acest motiv, sistemele de recunoaștere facială nu ar trebui să fie utilizate decât cu consimțământul prealabil al persoanei vizate.

Pontajele

În ceea ce privește sistemele de pontaj tradiționale, în practică se utilizează condica de prezență care de cele mai multe ori se regăsește la intrarea în firmă, într-un loc vizibil, eventual la recepție și sunt menționate numele și prenumele tuturor salariaților, ora la care au sosit și ora de plecare și semnătura. Deși evidența orelor de muncă ale salariaților este obligație legală a angajatorului stabilită prin Codul muncii, odată cu intrarea în vigoare a GDPR angajatorii trebuie să se preocupe de găsirea unor soluții alternative celor cu care deja s-au obișnuit.

Este greșită utilizarea unei astfel de condici din mai multe perspective. Pe de-o parte un tabel complet cu numele și prenumele fiecărui angajat lăsat la vedere este o încălcare a datelor personale din perspectiva vizitatorilor firmei, spre exemplu, al unui curier sau al unui client care se poate regăsi fără voia sa în proximitatea unei astfel de liste. Unul dintre riscurile la care sunt supuși salariați este inclusiv fotografierea listei și publicarea orelor de lucru, a datelor lor și a semnăturilor pe orice platformă, chiar și fără voia lor. Pe de altă parte, chiar și faptul ca salariații să aibă acces unii la programul altora, fără voia acestora, poate reprezenta o încălcare.



Exemplu „AȘA DA!”: Implementarea unui sistem de pontaj care are în vedere utilizarea unei aplicații de log-in și log-out care să

înregistreze electronic în funcție de fiecare user în parte programul de lucru al angajaților pe intervale orare și număr de ore.

O alternativă la sistemul de pontaj dat mai sus ca exemplu, pentru societățile mici care nu pot alocă un buget în acest sens, este de a alocă un cod numeric fiecărui salariat ce poate fi înscris pe condica fizică de prezență și care nu va mai putea identifica persoana angajatului decât împreună cu tabelul pe care departamentul de HR îl va păstra respectând principiul confidențialității.



Exemplu de amendă pentru utilizarea amprente:

În data de 30 aprilie 2020, o companie din Olanda a fost amendată pentru utilizarea amprente salariaților în vedere înregistrării timpului petrecut în companie. După investigație, Autoritatea olandeză pentru protecția datelor a ajuns la concluzia ca societatea nu ar fi trebuit să prelucraze amprente angajaților. Compania nu se poate baza pe un motiv de excepție pentru prelucrarea datelor cu caracter personal de acest tip și a fost amendată cu 725.000 de euro pentru acest lucru.

Datele biometrice, cum ar fi amprenta, sunt date personale speciale. O organizație nu poate utiliza date cu caracter personal speciale, cu excepția cazului în care există o excepție în acest sens din lege.

Monique Verdier, vicepreședinte al AP: „Această categorie de date cu caracter personal este protejată în plus de lege. Dacă aceste date ajung în mâini greșite, acest lucru ar putea duce la daune ireparabile. Cum ar fi șantajul sau fraudă de identitate. Nu se poate înlocui o amprentă, cum ar fi o parolă. Dacă lucrurile nu merg bine, impactul poate fi uriaș și poate avea efecte negative pe toată viața asupra cuiva”.

În acest caz, ar putea exista două excepții de la interdicția de utilizare a amprentelor: dacă persoanelor vizate, sunt solicitate consimțămintele explicite – sau dacă utilizarea datelor biometrice este necesară pentru autentificare sau securitate.

AP a concluzionat că această companie nu se poate baza pe una din aceste două excepții pentru colectarea, stocarea și utilizarea amprentelor digitale ale angajaților. Un angajator trebuie să ia în considerare dacă clădirile și sistemele de informații trebuie să fie atât de bine securizate încât acest lucru nu se poate face decât folosind (doar) biometrie. De multe ori nu va fi nevoie, deoarece există alternative bune. Un angajator solicită angajaților permisiunea de a prelucra amprenta lor? În principiu, acest lucru nu este permis. Angajații depind de angajatorul lor, astfel încât de multe ori, nu sunt în măsură să refuze.

B.C.B. „M. EMINESCU” IAȘI

ȘTIINȚE ECONOMICE



● Exemplu de amendă pentru prelucrarea datelor privind sănătatea:

Comisariatul pentru protecția datelor cu caracter personal din Cipru (Cypriot S.A.) a amendat LGS Handling Ltd, Louis Travel Ltd și Louis Aviation Ltd (grupul de companii Louis) pentru o sumă totală de 82.000,00 de euro, pentru lipsa bazei legale a instrumentului „Bradford Factor”, care a fost folosit pentru a nota concediile medicale ale angajaților.

Comisariatul a lansat o anchetă după ce o plângere a fost depusă de sindicatul angajaților.

Raționamentul din spatele sistemului automatizat Factor Bradford pentru notarea concediilor medicale a angajaților a fost faptul că absențele scurte, frecvente și neplanificate au dus la o dezorganizare mai mare a companiei decât la absențe mai lungi.

Data și frecvența unui concediu medical pentru o persoană, în măsura în care identitatea sa este direct sau indirect dezvăluită, presupun prelucrarea „categoriilor speciale de date cu caracter personal”, definite la art. 9 alin. (1) din GDPR. Furnizarea de date cu caracter personal unui sistem automat, notarea datelor utilizând „Factorul Bradford” și profilarea persoanelor în funcție de rezultate, este considerată prelucrarea datelor cu caracter personal; prin urmare, o astfel de operație de prelucrare trebuie să fie în conformitate cu principiile definite în GDPR.

Operatorul a efectuat o evaluare a impactului operațiunii de prelucrare și a fost trimis comisarului pentru consultare în timpul anchetei. Comisarul a fost de părere că operatorul nu a reușit să demonstreze prin evaluarea impactului că interesul său legitim predomină asupra intereselor, drepturilor și libertăților angajaților săi și, prin urmare, reducerea riscurilor a fost inadecvată.



Atenție! Studiile de impact pentru evaluare riscurilor la care pot fi supuse persoanele vizate se realizează înainte de a începe operațiunea de prelucrare a datelor cu caracter personal și abia după finalizarea evaluării și asumarea concluziilor se va demara o nouă prelucrare și nu invers.

Permisele de parcare

În incintele special amenajate cu locuri de parcare pentru angajați se utilizează frecvent permisele de parcare ce nu reprezintă documente ci pot

fi planșe printate cu numărul de înmatriculare al mașinii și denumirea firmei. Nu este necesar numele persoanei care conduce vehiculul, nu este necesar numărul de telefon al acestuia, precum niciun fel de date care să identifice persoana.

În ceea ce privește persoanele cu nevoi speciale, angajatorii trebuie să țină cont de faptul că permisele de parcare pentru persoanele cu handicap trebuie să îmbrace forma prevăzută de Ordinul nr. 223/2007 care conține fotografia, numele și prenumele titularului și semnătura acestuia sau alt însemn însă doar în ceea ce privește utilizarea locurilor publice de parcare. Pentru parcarile private, cum sunt cele din incinta unei clădiri de birouri, **NU ESTE NECESARĂ** implementarea unei legitimații de parcare care să dezvăluie datele privind starea de sănătate a persoanei vizate. Astfel, în ceea ce privește locurile special amenajate pentru angajații aflați în această categorie, angajatorul poate decide să ofere legitimații simple cu numărul de înmatriculare al mașinii și denumirea firmei și să se asigure doar de faptul de a pune la dispoziție locurile în mod nominal, spre deosebire de prima categorie care poate utiliza orice loc, fără o rezervare prealabilă.

Prelucrarea datelor cu caracter personal privind confesiunea religioasă

Prelucrarea religiei salariaților se realizează, în primul rând, pentru acordarea unor zile libere potrivit Codului muncii. Pentru ca acest lucru să se realizeze, angajații trebuie să declare confesiunea religioasă la angajare și ținând cont de particularitățile fiecărui cult religios, să beneficieze de zile libere în zilele de sărbătoare specifice.

Această prelucrare se face în temeiul legii și nu presupune consimțământul prealabil al salariaților, întrucât aceștia din urmă pot refuza să își dezvăluie apartenența la o altă religie decât cea comun întâlnită la nivelul României și să beneficieze de zilele libere stabilite cu caracter general.

Cu toate acestea, mai sunt și alte cazuri în care un angajat poate fi în situația de a dezvălui astfel de date, cum ar fi pentru acordarea unui meniu personalizat în cadrul petrecerilor organizate de firmă sau pentru masa decontată de angajator. Pentru respectarea convingerilor legate de anumite tipuri de alimente pe care anumite religii nu le consumă, angajatorul ar trebui să fie pus în tema cu privire la aceste aspecte, dar ca și în cazul zilelor libere, salariatul poate refuza să se exprime și nu va beneficia de meniul preferențial.

Un alt exemplu cu care se poate întâlni un angajator este acela în care salariații de o anumită confesiune religioasă au cerința unor pauze de masă sau pauze de lucru diferite de ale colegilor pentru a participa la rugăciune la anumite ore specifice ale zilei. Și în acest caz, beneficiul este acordat doar la cererea persoanei vizate și se recomandă consimțământul expres al salariatului care va înțelege faptul că de conduita sa specifică va depinde păstrarea confidențialității, dacă este cazul.

Prelucrarea imaginilor salariaților prin foto/video

Monitorizarea video a angajaților care utilizează mijloace de transport în comun puse la dispoziție de angajator

În calitate de operator de date cu caracter personal ce asigură transportul angajaților proprii sau după caz, ai societăților afiliate, angajatorul va putea prelucra imaginea colectată prin intermediul mijloacelor de supraveghere video ce vizează ca perimetru culoarul principal al mijlocului de transport, fiind vizibile și putând fi observate cu ușurință.

Scopul general în care se prelucrează imaginile video este asigurarea și menținerea securității și siguranței angajaților, bunurilor și valorilor societății, respectiv prevenirea incidentelor, inclusiv între șoferii microbuzelor/autobuzelor și angajații transportați.

Cu titlu de exemplu, datele pot fi prelucrate:

- pentru a verifica dacă în microbuzele/autobuzele societății sunt transportate alte persoane decât angajații firmei, ale căror acțiuni ar putea aduce atingere/au adus atingere drepturilor și/sau intereselor angajaților transportați,
- pentru a analiza și stinge conflictele dintre salariații transportați și șoferi,
- pentru a asigura securitatea bunurilor,
- pentru investigarea unor eventuale fapte de natură penală.

Categoriile speciale de date cu caracter personal (originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viață sexuală sau orientarea sexuală ale unei persoane fizice) nu sunt prelucrate prin intermediul mijloacelor de supraveghere video.

În aceste cazuri, este obligatorie efectuarea unei evaluări de impact care să stabilească gradul de risc la care sunt supuse persoanele vizate prin acest tip de prelucrare.

Camerele supraveghere amplasate în incinta de lucru a angajaților

Există două situații când angajatorul poate utiliza în mod legal camerele de supraveghere și ceea ce face diferența în stabilirea legalității este scopului prelucrării.

a. Atunci când angajatorul montează camere de supraveghere, deoarece, prin natura companiei și a bunurilor sale, este necesară această metodă de supraveghere pentru a monitoriza trasabilitatea unor produse, spre exemplu sau pentru a preveni distrugerea lor. În acest caz temeiul prelucrării este interesul legitim al operatorului, care trebuie desigur să fie echilibrat cu drepturile persoanelor vizate.

b. Atunci când camerele sunt amplasate pentru responsabilitate organizațională și civică sau siguranță publică și există o obligație a operatorului să instaleze un sistem de supraveghere video printr-un act normativ sau o lege.

Pentru ambele exemple de mai sus, informarea salariaților printr-o notă transmisă la angajare cumulată cu alte măsuri tehnice și organizatorice adecvate, sunt suficiente pentru respectarea drepturilor persoanelor vizate. Acest fapt va fi tratat mai pe larg în capitolul privind măsurile tehnice și organizatorice.

De ce nu se recomandă consimțământul persoanelor vizate ca temei de prelucrare a datelor prin mijloace de supraveghere video?

În cazurile prevăzute la punctele a și b nu este nevoie de consimțământul persoanelor vizate pentru că nu este necesar. Interesul legitim al operatorului și obligațiile legale sunt suficiente ca temeiuri de prelucrare și nu se impune solicitarea consimțământului salariaților pentru acest tip de prelucrare.

Cu toate acestea, dacă angajatorul nu justifică niciunul dintre temeiurile prevăzute mai sus, am crede că putem solicita consimțământul și acesta va substitui orice alt temei legal, însă nu este așa. E bine cunoscut faptul că raportul angajator-angajat este unul disproporționat și un sistem de monitorizare video, deși poate fi intruziv și abuziv, poate fi acceptat de către persoanele vizate din teama de a își pierde locul de muncă dacă nu se supun regulilor firmei.

O astfel de abordare este sever criticată de specialiștii în domeniu, precum și de către reprezentanții autorităților de supraveghere din România și din Europa și nu trebuie să reprezinte o opțiune pentru operator. În plus, prin aptitudinea consimțământului de a fi retras, există oricând riscul de conflict între a păstra sau nu un sistem de supraveghere.

Exemple de interes legitim:

- Firmele care au ca obiect de activitate prelucrarea lemnului și cherestelei și care au amplasate camerele de supraveghere în depozite precum și în incinta fabricii pentru a preveni incendiile.
- Unitățile comerciale care vând produse inflamabile sau combustibil de asemenea se pot prevala atât de interesul legitim precum și de siguranța publică. Deși în aparență nu s-ar justifica amplasarea camerelor și în incinta unde se desfășoară activitatea de birou, dacă perimetrul este de așa natură încât va preveni riscurile la care se supun salariații care traversează zonele respective, este legitim.
- Benzile de producție alimentară pot fi supravegheate video pentru siguranța alimentară și a consumatorilor de respectivele produse ș.a.



Atenție! Nu pot fi utilizate imaginile de pe camerele de supraveghere amplasate pentru scopurile amintite mai sus în vederea analizei programului salariaților, a respectării orelor de lucru și pentru a fi utilizate într-o eventuală cercetare disciplinară pentru motive de întârziere.

Nu este permisă nici utilizarea capturilor de ecran pe care le pot surprinde camerele de supraveghere, pentru a dovedi o conduită neconformă a unui salariat, în afara cazului în care acest lucru nu este solicitat în mod expres de către persoana vizată însăși care poate solicita utilizarea unei astfel de probe în apărarea sa.



• **Exemplu de amendă:** C.N.I.L. (Autoritatea de supraveghere din Franța) a impus o sancțiune de 20.000 de euro împotriva companiei UNIONTRAD COMPANY pentru utilizarea unui sistem de supraveghere video care a plasat angajații săi sub supraveghere constantă.

De asemenea, a emis o dispoziție prin care obligă compania să ia măsuri pentru a asigura trasabilitatea accesului la mesajele profesionale partajate. Amenda a fost însoțită de o penalitate de 200 de euro pe zi de întârziere la sfârșitul unei perioade de două luni de la notificarea acestei deliberări.

Publicarea fotografiilor și videoclipurilor de la activitățile individuale sau colective profesionale și extra-profesionale

Principalul mod în care sunt prelucrate imaginile salariaților unei companii și cel mai frecvent de altfel este prin publicarea imaginilor pe

site-ul companiei la secțiunea destinată prezentării echipei. Deși în practica anterioară intrării în vigoare a GDPR, prin simplul fapt al participării unui salariat la sesiunea foto pentru a fi postat pe site se subînțelegea acordul acestuia, din 25 mai 2018 nu mai este suficient.

Ca o bună practică de implementat în cadrul unei societăți se recomandă crearea unui formular de consimțământ adresat angajatului, prin care se specifică în mod expres faptul că respectiva fotografie va fi publicată pe site și în ce scop, iar acesta din urmă va avea posibilitatea de a se exprima în mod informat dacă este de acord sau nu. În cazul în care nu se obține consimțământul angajatului, compania nu va publica fotografia ci va putea recurge la publicarea unui chenar simplu sub care va trece doar numele și prenumele, iar în cazul în care salariatul nu va fi de acord nici cu publicarea acestor date, angajatorul va publica eventual doar funcțiile existente în departamentul respectiv.

Un alt mod de a proceda în afara formularului de consimțământ ca document de sine stătător poate fi solicitarea unei fotografii în vederea publicării pe site, cu explicațiile de rigoare în corpul unui e-mail în care se va menționa că, prin răspunsul pozitiv, scris și explicit la e-mail însoțit de o fotografie se va parcurge procesul de luare a consimțământului persoanei vizate.



Exemplu „AȘA NU!”: Preluarea unei fotografii a salariatului de pe un profil public de socializare și publicarea pe web-site fără acordul prealabil al acestuia.

Sau

Păstrarea fotografiei angajatului la sesiunea destinată pe web-site a echipei, deși colaborarea a încetat și persoana vizată nu mai face parte din companie.

Pentru evitarea unor astfel de situații ar trebui să existe cel puțin o persoană desemnată din departamentul de HR care să se ocupe de verificarea periodică a fotografiilor și a numelor persoanelor din echipă și să ordone ștergerea din oficiu atunci când încetează un contract de muncă. Dacă acest lucru nu va fi posibil, prin exercitarea dreptului la ștergere (dreptul de a fi uitat) al persoanei vizate, angajații care părăsesc o companie pot face o cerere scrisă adresată angajatorului prin care să solicite în mod expres acest lucru, urmând ca firma să dea curs într-un termen rezonabil de timp.

Un alt caz în care pot fi prelucrate imaginile foto sau video ale salariaților este publicarea lor în urma participării la o activitate lucrativă de

tip workshop sau seminar pe site-ul companiei sau chiar și pe rețelele de socializare. În scopul diseminării informațiilor despre proactivitatea firmei se întâmplă de foarte multe ori ca aceste tipuri de instruiți să facă obiectul unei ședințe foto. Cu toate acestea, ca și în cazul prezentat mai sus, nu pot fi utilizate astfel de imagini fără consimțământul expres al salariaților.



Exemplu „AȘA NU!”: O firmă care activează în domeniul producției auto a fotografiat un program de instruire a salariaților în domeniul sănătății și securității în muncă și au fost surprinse imagini cu persoane vizate care învățau cum să acorde primul ajutor în cazul unui accident de muncă. În acele imagini erau prezentate persoane care simulau resuscitarea prin respirație gură la gură și una dintre persoanele vizate a acuzat angajatorul că i-a fost încălcat dreptul la imagine precum și la viața privată.



Exemplu „AȘA DA!”: Lista lui Moș Crăciun poate fi un motiv de încălcare a drepturilor persoanelor vizate, în special pentru că este vorba de persoane vizate care sunt minori. Pentru a preveni o conduită neconformă, atunci când angajatorul organizează o petrecere pentru copiii salariaților din firmă, o bună practică este de a solicita consimțământul părinților pentru a colecta sexul și vârsta copiilor precum și numele și prenumele acestora pentru a le cumpăra cadouri la sărbătorile de iarnă. Pe același consimțământ se va lua în calcul și acordul pentru prelucrarea imaginii celor mici prin fotografierea și publicarea imaginilor pe site-ul companiei sau pe rețelele de socializare ale firmei.

Și în cazul team building-urilor sau a activităților de voluntariat și recreative, se pune problema filmărilor și fotografiilor persoanelor vizate, astfel că în politica internă de prelucrare a datelor la nivelul departamentului HR se recomandă o procedură de verificare a tuturor acestor acțiuni ale firmei anterior desfășurării lor, cu participarea activă a angajaților care vor fi informați cu privire la politica firmei precum și cu privire la drepturile pe care le au față de respectivele prelucrări.

Comentariu: În ceea ce privește joburile care prin natura lor implică imaginea persoanelor vizate, cum ar fi modelele pentru fotografiile utilizate de un magazin online care vinde haine sau accesorii purtate de persoane, animatorii sau persoanele care joacă un rol într-un videoclip de prezentare de servicii sau produse, lectorii pentru cursuri on-line care urmează să fie distribuite pe diverse platforme, ș.a. clauzele privind prelucrarea imaginii

se vor însera în contractul individual de muncă printr-o anexă care stabilește de la începutul raporturilor contractuale nivelul de risc la care se supune persoana vizată prin expunerea publică, faptul că natura profesiei este astfel concepută și are componenta prelucrării imaginii și că anumite drepturi pot fi îngădite, cum ar fi dreptul de a fi uitat.

În aceste cazuri se recomandă inclusiv semnarea unui acord privind cedarea drepturilor la imagine, contract ce are menirea de a stabili cadrul și limitele în care poate fi utilizată fotografia sau filmulețul cu persoana în cauză.

Administrarea dosarelor de personal. Tipuri de date prelucrate.

Bune practici

În cadrul firmelor se întocmesc, se gestionează și se actualizează ori de câte ori este necesar dosarele personale ale angajaților.

Procedura este îndeplinită de către Departamentul de Resurse Umane prin angajații săi care răspund de corectitudinea și valabilitatea documentelor existente la dosarul de personal, precum și de prelucrarea datelor cu caracter personal, conform Regulamentului nr. 679/2016.

La fiecare angajare este necesară întocmirea dosarului personal al salariatului în cauză. Întocmirea dosarului se face cu cel puțin o zi lucrătoare înainte de începerea efectivă a activității salariatului în cadrul companiei.

De întocmirea și completarea corectă a dosarelor profesionale răspund angajații Departamentului de Resurse Umane, aceștia urmând să menționeze pe coperta dosarului numele, prenumele celui care a întocmit și/sau verificat dosarul și data acestei operațiuni. Completarea ulterioară a dosarului de personal cu alte documente se va face, în măsura în care acest lucru va fi posibil, de către același angajat care l-a întocmit, certificând totodată corectitudinea actelor întocmite și înregistrarea datelor în REVISAL atunci când se impune.

De asemenea, se vor înmâna salariatului, sub semnătură de primire sau prin poștă cu confirmare de primire, exemplarele proprii ale contractului individual de muncă, actelor adiționale, deciziilor de sancționare și/sau de modificare a contractului de muncă, orice alte documente prevăzute de legislația muncii. Dovezile de predare a respectivelor documente vor fi păstrate la dosarul personal al angajatului în cauză.

Dosarul profesional va cuprinde, în mod obligatoriu, la momentul angajării cel puțin următoarele tipuri de documente care conțin date cu caracter personal:

- Cererea de angajare;
- Contract individual de muncă;
- Fișa postului;
- Act adițional clauza de formare profesională – dacă este cazul;
- Act adițional clauza de confidențialitate – dacă este cazul;
- Fotocopie act identitate valabil la data întocmirii dosarului de personal;
- Fotocopie act stare civilă – dacă este cazul;
- Fotocopii certificate de naștere copii minori – dacă este cazul;
- Aviz medical/fișă de aptitudine care să ateste o stare de sănătate corespunzătoare exercitării funcției;
- Fotocopii acte de studii, atestări profesionale;
- Fotocopii certificate de participare la cursuri de instruire sau perfecționare;
- Recomandări de la locurile de muncă anterioare (în anumite situații);
- Curriculum Vitae;
- Declarație privind alegerea persoanele în întreținere în vederea calculării deducerilor personale și documente justificative (certificate de naștere, căsătorie, declarații, adeverințe), înscrierea la Casa de Asigurări de Sănătate;
- Adeverința care să ateste stagiul de cotizare, de la angajatorul anterior (dacă este cazul);
- Alte declarații privind deducerile personale.

Pe parcursul derulării raporturilor contractuale de muncă, dosarul personal se va completa, acolo unde este cazul cu:

- Acte adiționale la contractul de muncă prin care se modifică funcția, locul muncii, salariul, perioada contractuală, norma de lucru, sporurile, indemnizațiile, alte adaosuri, condițiile de muncă, durata muncii, durata concediului de odihnă anual; fișa postului;
- Deciziile de delegare, detașare;
- Deciziile de desemnare în comisii;
- Cererile și deciziile de suspendare ale raporturilor de muncă;
- Decizii de sancționare;
- Deciziile de încetare a raporturilor de muncă;
- Nota de lichidare (după caz);
- Rapoarte de evaluare;

- Documente care completează, modifică, actualizează alte documente existente la dosarul profesional;
- Comunicarea prin care salariatul este informat și consimte la prelucrarea datelor cu caracter personal.

În condițiile legii, au dreptul să acceseze datele cu caracter personal și profesional înscrise în dosarul personal următoarele persoane:

- Angajatul în cauză;
- Angajații din Departamentul de Resurse Umane;
- Analistii sistemelor de salarizare;
- Directorii unității în subordinea căruia se află angajatul respectiv;
- Persoanele împuternicite ale unor autorități sau instituții publice cu atribuții de control;
- Președintele și/sau membrii comisiei de disciplină;
- Organele de cercetare penală;
- Orice alte instituții către care angajatorul are obligația de a furniza date cu caracter personal conform legislației în vigoare.

Datele cuprinse în dosarul profesional sau în registrul de evidență a salariaților pot fi rectificate sau completate în următoarele situații:

- La solicitarea scrisă și motivată a angajatului în baza drepturilor garantate de Regulamentul 2016/679;
- La solicitarea scrisă și motivată a Directorului/managerului de resurse umane, după caz, a persoanei care are atribuții cu privire la evidența personalului, prevăzute în fișa de post, cu aprobarea șefului ierarhic și cu înștiințarea salariatului în cauză;
- În baza unei hotărâri judecătorești definitive;
- Din dispoziția altor autorități ale statului.

De asemenea, datele din dosarul personal ale salariatului trebuie trecute în REVISAL și raportate la ITM, conform dispozițiilor legale în materie.

Dosarele salariaților vor fi păstrate fizic într-un dosar cu cheie, la care nu vor avea acces persoane care nu au fost autorizate în prealabil de către conducerea societății sau a departamentului de resurse umane.

Eliberarea adeverințelor care atestă corectitudinea datelor. Scrisori de recomandare

Atât în cursul derulării unui raport de muncă, precum și la încetarea sau după încetarea acestuia, cade în sarcina angajatorului să elibereze diferite tipuri de documente către salariat sau către terțe părți care le solicită.

! • **Exemplu 1:** Adeverința care atestă vechimea în muncă și care este eliberată împreună cu un extras din registrul de evidență al salariaților la încetarea raporturilor de muncă. Aceste documente se eliberează direct salariatului și se vor folosi metode de comunicare care nu permit accesul persoanelor neautorizate la conținutul lor. Nu vor fi înmânate în niciun caz unui coleg sau prieten și nici nu se lasă la recepția firmei pentru a fi ridicate de salariat, în afara cazului în care se folosește un plic sigilat și această metodă de comunicare este solicitată în scris de persoana vizată.

! • **Exemplu 2:** Adeverința privind veniturile realizate de salariat eliberată la solicitarea acestuia pentru a fi folosită în vederea achiziționării unui credit. Acest document se transmite fie direct persoanei vizate, fie unității bancare, la solicitarea expresă, în scris a salariatului. O bună practică este utilizarea unui canal de comunicare securizat și verificarea, anterior transmiterii documentului, a măsurilor tehnice și organizatorice pe care le are implementate terțul.

! • **Exemplu 3:** Scrisoarea de recomandare oferită salariatului pentru a putea fi utilizată la o nouă angajare care poate conține date privind conduita acestuia la locul de muncă, situația abaterilor disciplinare pe care le-a avut dacă se solicită clarificări și în acest sens, cursurile de formare profesională la care a participat persoana vizată, ș.a.m.d.

Există și situația particulară în care noul angajator sună pentru referințe direct, sau transmite un e-mail prin care solicită informații privind activitatea desfășurată de salariat pe durata desfășurării colaborării. Pentru a da curs unei astfel de solicitări, este necesar consimțământul prealabil al salariatului, pentru a nu îi fi încălcate drepturile.

! • **Exemplu 4:** Adeverința de salariat pentru medicul de familie este solicitată de angajat în scopul acordării anumitor tipuri de concedii și indemnizații. Printre acestea se numără cele pentru incapacitatea temporară de muncă, cauzată de boli obișnuite sau de accidente în afara muncii, și cele acordate pentru accidente de muncă sau boli profesionale. Adeverința se acordă și în cazul concediilor medicale și al indemnizațiilor pentru maternitate, pentru îngrijirea copilului bolnav sau pentru cazuri de risc maternal.

Prelucrarea datelor în timpul unei cercetări disciplinare

Cercetarea prealabilă a salariaților reprezintă o procedură obligatorie în vederea acordării sau nu a unei sancțiuni și este prevăzută de Codul muncii, iar datele privind faptele săvârșite de angajat sunt confidențiale, reprezintă date cu caracter personal, dat fiind faptul că acestea pot conduce la identificarea persoanei în anumite cazuri și pot face obiectul unei ample analize din perspectiva GDPR.

Documente implicate în proces:

- Adrese sau referate întocmite de alți angajați, precum departamentul de HR, superiorul direct, un coleg de echipă sau chiar administratorul societății,
- Convocarea la cercetarea disciplinară,
- Procesul verbal din ședința de cercetare disciplinară,
- Decizia de sancționare.

Pe toată durata conflictului, de la apariția faptei încadrate de angajator ca abatere disciplinară și până la emiterea deciziei de sancționare, sunt implicate mai multe persoane care iau contact cu informații despre persoana salariatului, pot avea acces la dosarul de salariat, pot adresa întrebări altor colegi de echipă sau reprezentantului salariaților și, nu în ultimul rând, desfășoară o anchetă care poate pune persoana vizată într-o împrejurare riscantă din punctul de vedere al datelor cu caracter personal.

Ca o bună practică în companie, se recomandă crearea unei proceduri disciplinare clare pe care angajatorul o va menționa în regulamentul intern al companiei și se va asigura de faptul că implicațiile din punct de vedere GDPR sunt controlate.

Comisia de disciplină trebuie să fie formată doar din persoane care au luat la cunoștință despre faptul că datele personale ale salariatului trebuie protejate pe toată durata procesului de cercetare precum și după încetarea acesteia și vor fi instruite în acest sens. Nu este permisă delegarea unor astfel de atribuții către persoane care nu au o înțelegere profundă a domeniului protecției datelor, care ar putea divulga fără permisiunea salariatului anumite informații.

De asemenea, nu este permisă transmiterea de informații către asociații firmei, dacă nu este necesar acest lucru în cazul în care aceștia sunt persoane juridice din alte state și cu privire la care nu există informații că ar avea măsurile tehnice și organizatorice necesare pentru a asigura protecția datelor.



Important! Cercetările disciplinare, precum și rezultatul lor nu ar trebui să se desfășoare nici măcar cu informarea altor salariați care nu sunt direct implicați în proces. Divulgarea de date personale prin publicarea rezultatului pe platforme de comunicare este interzisă cu strictețe și acest lucru este valabil atât pentru angajator, cât și pentru participanții la comisia de disciplină.

Aceleași reguli se aplică și în cazul anchetelor desfășurate de angajator pentru cazuri de hărțuire sau discriminare despre care ia cunoștință în cadrul companiei și, precum în situația expusă anterior, se va întocmi o procedură specială pentru aceste situații pentru a avea o gestiune legală a situației.

De asemenea, chiar încălcările în ceea ce privește protecția datelor cu caracter personal reprezintă ele însele abateri disciplinare pe care angajatorul le poate menționa în regulamentul intern al societății pentru a putea atrage răspunderea salariatului.



Exemplu „AȘA DAI”: Toate documentele ce țin de anchetele disciplinare, anti-hărțuire sau anti-discriminare se vor păstra separat de dosarele de salariat sau arhivate în mod corespunzător, deoarece nu există necesitatea ca acestea să se regăsească în mod fizic la dosare. Coordonatorul departamentului HR ar trebui să ia în considerare ca doar în cazuri excepționale să prezinte astfel de înscrisuri, cum ar fi în eventualitatea unui litigiu, altfel se poate ca în mod accidental să apară un incident de securitate nedorit în firmă.

Mijloacele de comunicare utilizare cu și de către salariați

Pentru controlul situațiilor neconforme și armonizarea practicilor în interiorul unei societăți, este necesară stabilirea unor mijloace de comunicare pe care să le utilizeze atât angajații între ei, precum și cu terții (clienți, furnizori, parteneri de afaceri ș.a.m.d.).

În concret, procedura în sine constă în stabilirea limitativă a ce dispoziitive se utilizează la nivel de companie și ce canale de comunicare sunt permise, cu verificarea prealabilă că îndeplinesc cerințele de securitate a informației.

! **Exemplu 1:** Toți angajații societății vor folosi aceeași aplicație pentru transmiterea e-mailurilor și aceeași găzduire de web-mail. De asemenea, se vor utiliza exclusiv telefoane de serviciu și laptopuri de serviciu sau tablete, iar societatea nu va permite abaterea de la aceste reguli.

! **Exemplu 2:** Va fi interzisă prin regulamentul intern salvarea în telefonul de serviciu sau în laptopul de serviciu de documente sau fotografii personale ale angajaților. Se va preciza faptul că încălcarea acestei reguli va atrage după sine și exonerarea angajatorului de orice responsabilitate în situația încălcării drepturilor la viața privată a salariatului, deoarece nu vor exista măsuri tehnice și organizatorice de protecție a unor astfel de date personale.

Într-o speță recentă, un angajat al unei firme a solicitat acces la datele personale pe care le avea salvate în laptopul de serviciu, în condițiile în care a fost concediat și i s-a restricționat accesul la laptop și telefon mobil. Acesta a precizat că, în virtutea dreptului de acces și a dreptului de a fi uitat, ar trebui ca operatorul să îi permită să verifice personal ce informații salvase pe dispozitivele respective și să dispună el singur de ștergerea lor pentru a se asigura că nimeni nu va mai avea acces la respectivele informații.

O bună practică din partea operatorului este resetarea dispozitivelor cu ștergerea completă a tuturor informațiilor de pe echipamentele electronice și emiterea unui proces-verbal în acest sens.

! **Exemplu 3:** Pentru prevenirea unei breșe de securitate, toți angajații vor comunica intern doar prin aplicații de tipul Skype sau Whatsapp pentru desktop care vor fi logate la adresele de e-mail profesionale și la numerele de telefon de serviciu.

BUNE PRACTICI ÎN DEPARTAMENTELE DE MARKETING, VÂNZĂRI ȘI CLIENT SUPPORT

Este mai important să faci ce este corect din punct de vedere strategic, decât ce este imediat profitabil.

Philip Kotler

Principiu de respectat în orice circumstanțe

Oricând datele unei persoane sunt colectate în scopuri de Marketing, aceasta va fi informată în mod corespunzător privind activitatea de prelucrare a datelor sale cu caracter personal, inclusiv cu privire la dreptul său de a interzice oricând utilizarea datelor sale personale în scopuri de Marketing.

Diferită de prelucrarea datelor angajaților companiei (prelucrare care se face eminentemente în scop legal sau legitim), prelucrarea în scop de Marketing sau Vânzări naște cele mai multe controverse și cele mai multe „inovații”. Pentru unele companii bazele de date și imboldul dat clienților pentru a cumpăra reprezintă esența existenței lor pe piață (magazinele online, companiile care vând cursuri, organizatorii de evenimente etc.).

Acest lucru nu înseamnă că prelucrarea datelor nu se poate face în mod corect, respectând confidențialitatea și intimitatea consumatorului.

Foarte multe persoane se întreabă ce este profilarea și dacă poate fi făcută în mod legal. Mulți fac această profilare și nu își dau seama că se încadrează aici, iar o parte sunt foarte înverșunați împotriva profilării, susținând că nimeni nu are dreptul de a urmări preferințele unei anumite persoane. Vom dezbate și această problemă a profilării în prezentul capitol.

Departamentul de Marketing

1.1.1. Datele cu caracter personal prelucrate în scop de Marketing

Departamentul de Marketing din companie (sau societatea parteneră care se ocupă de publicitatea companiei – imputernicită în acest sens) colectează și prelucrează în general următoarele date cu caracter personal:

- Numele și prenumele persoanei vizate;
- Adresa de e-mail a persoanei vizate;
- Denumirea conturilor de social media;

- Adresa de domiciliu și eventual alte date din Cartea de identitate (exemplu: în cazul organizării de concursuri în scop publicitar când se colectează datele câștigătorilor)

- Adresa indicată de persoana vizată (în acest caz discutăm de adresa comunicată expres de client pentru livrarea premiului în cazul în care societatea organizează vreun concurs);

- Adresa IP (în acest caz, este vorba doar despre accesarea adresei IP, fără alte operațiuni);

- Fotografii ale persoanelor vizate, încărcate de acestea pe platformele de socializare (în situația organizării concursurilor de tipul „Cea mai bună fotografie”);

- Numărul de înmatriculare al mașinii (exemplu: reducere la prețul benzinei sau un cadou pentru mai multe vizite la respectiva benzinărie).

Majoritatea companiilor prelucrează doar o parte din aceste date – mai sus am enumerat cele mai comune tipuri de date colectate în general de departamentul de Marketing.

Alte date rareori sunt prelucrate în scop de marketing, deși uneori se mai pot prelucra și alte date cu caracter personal, cum ar fi data nașterii clienților sau alte informații de tipul (fumează sau nu, călătorește des sau nu etc.).

Unele companii prelucrează data de naștere pentru a putea oferi cadouri/discount-uri de ziua de naștere sau atunci când organizează anumite concursuri publicitare dedicate doar persoanelor majore – dar această dată, aparent neimportantă poate fi parte a profilării clientului respectiv.

Același lucru se poate spune despre sexul persoanei – este util, de exemplu, pentru un magazin de pantofi să colecteze date privind sexul persoanei pentru a putea trimite noutăți relevante – pe un bărbat pasionat de sporturi extreme rareori l-ar interesa ultima colecție de pantofi cu toc, de exemplu.

Rareori sunt prelucrate date speciale (cum ar fi starea de sănătate) de către Departamentul de Marketing sau de către Departamentul de Vânzări. Poate doar atunci când se promovează anumite medicamente, dispozitive medicale sau aparatură medicală.

Exemplu de prelucrare de date speciale în scop de marketing: campanie publicitară dedicată celor care folosesc scaune cu roțile (fotolii rulante) în care se colectează date despre handicapul persoanei pentru a fi înscrise la o tombolă publicitară.

Descrierea activităților de marketing la nivel intern

Activitatea internă de marketing este realizată fie intern (departamentul de Marketing al companiei), fie extern (colaborarea cu una sau mai multe agenții de publicitate/PR/media), fie atât intern, cât și extern.

În cazul în care există un departament de marketing în cadrul societății, este recomandat să se întocmească o procedură specială pentru acest departament (care să conțină inclusive o listă de „AȘA DA!” și „AȘA NU!”), pentru a fi mai ușor pentru angajați să înțeleagă ce au de făcut.

În cazul în care departamentul de marketing este externalizat (către o agenție de publicitate/media), atunci trebuie foarte clar stabilit prin contractul încheiat între cele două societăți (sau printr-un act adițional redactat special în acest scop) cine păstrează datele, pentru cât timp, cui le poate transmite, în ce condiții etc. Bineînțeles, având în vedere faptul că societatea este cea care deține aceste date în mod legal, va răspunde pentru eventualele folosiri nelegale și pentru eventualele breșe de securitate.

Este foarte importantă alegerea societății cu care se colaborează, administratorii societății având o obligație legală de a verifica societatea de publicitate, nu doar din punctul de vedere al rezultatelor și al eticii, ci și din punct de vedere al respectării normelor privind securitatea datelor cu caracter personal.

În ceea ce privește modalitățile de promovare – ne putem referi la două mari categorii: online și offline. Cele mai multe companii aleg să se promoveze prin ambele modalități, existând astfel prelucrări de date și prin marketingul/vânzările online și prin marketingul/vânzările offline.

În ceea ce privește promovarea offline, aceasta se face de obicei prin următoarele modalități:

- pliante de prezentare a produselor;
- produse personalizate (cum ar fi tricourile personalizate);
- cărți de vizită;
- sponsorizări;
- produse oferite prin intermediul unor concursuri cu premii;
- participare la evenimente;
- organizarea de evenimente de prezentare;
- apariții în pliante, reviste ale partenerilor;
- mostre oferite gratuit;
- poziționarea de diferite afișe outdoor sau indoor (în lifturi sau în diferite alte locuri unde se permite această practică)

Din punctul de vedere al prelucrării datelor cu caracter personal, departamentul de marketing/societatea împuternicită trebuie să acorde

atenție sporită organizării de evenimente (în acest caz se colectează și prelucrează foarte multe date) și organizării concursurilor în scop publicitar (și în acest caz se colectează foarte multe date cu caracter personal).



• **Util de folosit:** În manualul (Procedura de lucru) dedicat departamentului de marketing ar trebui să se regăsească mențiuni concrete privind organizarea de evenimente și organizarea de concursuri – ce obligații au angajații, unde trebuie stocate acele date, cine are acces la ele etc. (vom detalia acest subiect în capitolul privind procedurile).

Promovarea online se poate face în următoarele modalități:

- Gestionarea rețelelor de socializare (Facebook, Instagram, Youtube, LinkedIn, TikTok etc.);
- Gestionarea Website-ului (inclusiv anunțuri plătite pe Google – Google Adwords);
- Publicitate în mediul online (pe site-urile partenerilor, site-uri de anunțuri, evenimente online, publicitate în emisiunile difuzate online);
- Promoții/concursuri în mediul online;
- Trimiterea de newslettere pe email/Whatsapp.

La fel ca în cazul publicității offline, organizarea de concursuri presupune colectarea multor date (inclusiv imagini – fotografii câteodată). Dar cele mai multe date se colectează prin intermediul website-ului și a cookies-urilor – prin aceste instrumente putându-se și profila consumatorii.

Scopurile prelucrării datelor cu caracter personal în departamentul de marketing

Dacă discutăm de o colaborare cu o societate de publicitate, în cadrul relației Operator-Împuternicit, scopurile prelucrării datelor cu caracter personal pot fi:

- Statistica;
- Trimiterea de Newsletter;
- Promovare generală reprezentată de concursuri/campanii;
- Organizarea de evenimente;
- Administrarea bazelor de date ale companiei.

În cazul în care nu există un împuternicit, scopul prelucrării va fi evident promovarea societății/publicitatea produselor sau serviciilor acesteia.

Util de folosit! Persoana fizică va trebui informată despre scopul prelucrării, dar nu este obligatoriu ca acesta să fie menționat așa: „scop de marketing”/ „scop publicitar” – puteți informa astfel: „ în scopul informării despre ofertele noastre” sau „ în scopul anunțării apariției de noi produse similare cu cel achiziționat de dvs.” sau „în scopul informării despre noutățile care apar în materie”.

În acest fel, suntem convinse că rata celor care acceptă informarea periodică (prin newsletter) va fi mai mare decât dacă ar fi specificat „scop publicitar”, deși până la urmă înseamnă același lucru.

Legalitatea prelucrării datelor cu caracter personal (temeiuri legale) de către departamentul de marketing

Ținând cont de scopurile urmărite prin prelucrarea datelor cu caracter personal, primul pas în evaluarea conformității unei prelucrări de date este determinarea temeiului juridic în baza căruia se face prelucrarea. Fără un temei juridic corect identificat, prelucrarea încalcă prevederile GDPR.

După cum am discutat mai sus, prelucrarea datelor cu caracter personal se poate realiza în mod legal numai dacă se bazează pe unul dintre temeiurile juridice prevăzute la art. 6 alin. (1) din Regulament, respectiv:

- consimțământul persoanei vizate;
- prelucrarea este necesară pentru încheierea sau executarea unui contract;
- prelucrarea este necesară pentru îndeplinirea unei obligații legale;
- prelucrare este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- prelucrare este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
- prelucrare este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate.

Pentru majoritatea persoanelor din departamentele de Marketing (de altfel și pentru departamentele de Vânzări) din societăți, relevant ar fi doar temeiul legal legat de consimțământul persoanei vizate.

Noi vă atragem atenția și asupra ultimului temei legal, interesul legitim – pe care se pot întemeia multe acțiuni ale societății reducând costurile acesteia legate de obținerea, dovedirea sau ștergerea consimțământului.



De reținut!

- Alegerea temeiului de prelucrare trebuie făcută corect de la început, schimbarea ulterioară a temeiului, fără justificare adecvată, fiind echivalentă cu o neconformitate.

- Alegerea temeiului de prelucrare trebuie corelată cu scopul prelucrării (în acest capitol discutăm doar de scop de marketing și vânzări)

În ceea ce privește cele două departamente (Marketing și Vânzări), avem astfel două temeuri legale pe care putem să întemeiem o prelucrare de date:

Prelucrarea se bazează pe consimțământul persoanei vizate

Consimțământul înseamnă a oferi persoanelor posibilitatea de a alege (dacă și pentru ce perioadă vor să primească anunțuri publicitare) și a controla (oricând persoanele vizate pot solicita încetarea primirii de newslettere sau de mesaje publicitare).

Legea nr. 506/2004 și Legea nr. 365/2002 privind comerțul electronic:

„Este interzisă efectuarea de comunicări comerciale prin utilizarea unor sisteme automate de apelare și comunicare care nu necesită intervenția unui operator uman, prin fax ori prin poșta electronică sau prin orice altă metodă care folosește serviciile de comunicații electronice destinate publicului, cu excepția cazului în care abonatul sau utilizatorul vizat și-a exprimat în prealabil consimțământul expres pentru a primi asemenea comunicări”.

Efectuarea de comunicări comerciale prin poșta electronică este interzisă, cu excepția cazului în care destinatarul și-a exprimat în prealabil consimțământul expres pentru a primi asemenea comunicări.

În cazul în care prelucrarea datelor se bazează pe consimțământ, operatorul trebuie să poată demonstra faptul că persoana vizată și-a dat consimțământul.

Vom detalia acest aspect în alt capitol, însă este un fapt care trebuie subliniat – nu este suficient ca acordul să fie verbal (în cadrul unui eveniment, de exemplu, sau la un târg unde se colectează foarte multe cărți de vizită). Este obligatoriu ca persoana vizată fie să semneze (utilizând o semnătură electronică sau una olografă, de mână), fie să apese pe butonul de „accept” („vreau să primesc comunicări publicitare”), iar softul să poată reține și operatorul să poată demonstra acordul dat.

Obținerea unui consimțământ valabil potrivit GDPR nu este o sarcină ușoară, de aceea recomandarea noastră este să acordați o atenție sporită acestui aspect, iar noi vom pune accent în următoarele pagini pe condițiile pe care trebuie să le îndeplinească consimțământul pentru a fi legal.

Consimțământul este definit în art. 4 pct. 11 din Regulament drept „orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate”.



Exemple de consimțământ:

Confirmă că ai citit și ești de acord cu termenii și condițiile site-ului și cu colectarea datelor tale pentru a primi newslettere de la noi:

X (prebifat) Sunt de acord

Nu sunt de acord

Ne-ar plăcea să vă trimitem ofertele noastre promoționale și noutăți în domeniu.

Vă rugăm să precizați dacă doriți să primiți aceste noutăți și/sau oferte pe email:

Sunt de acord

Nu sunt de acord

Condițiile pe care trebuie să le îndeplinească consimțământul

Pentru a fi valabil, consimțământul trebuie să îndeplinească cumulativ următoarele condiții:

- să fie dat în mod liber;
- să fie specific;
- să fie informat;
- să fie lipsit de ambiguitate;

Consimțământul copiilor este supus unor condiții suplimentare și vom discuta mai jos despre acest aspect.

a. Consimțământul trebuie să fie dat în mod liber

Potrivit Grupului de lucru „art. 29”, consimțământul trebuie să fie o alegere reală pentru persoana vizată. Dacă persoana nu are o alegere reală, se simte obligată să își dea consimțământul sau urmează să suporte consecințe negative dacă nu își dă acordul, consimțământul nu este valabil.

Utilizarea unui serviciu condiționată de acordarea consimțământului este permisă doar dacă prelucrarea datelor este necesară pentru executarea respectivului contract



● **Exemplu de condiționare permisă:** trimiterea pe e-mail a unei opinii fiscale gratuite după ce solicitantul a completat un formular în acest sens, dar nu este permis să se solicite și alte date care nu sunt necesare (număr de telefon, nume, adresă etc.) și nici ca ulterior să se trimită alte mesaje publicitare și nici păstrarea adresei de email pentru alte scopuri.

Exemplu oferit de Grupul de lucru „art. 29”:

„O aplicație pentru editarea fotografiilor solicită utilizatorilor să aibă locația GPS activată pentru utilizarea serviciilor, datele privind geolocalizarea fiind colectate în scopuri de publicitate comportamentală. Geolocalizarea nu este necesară pentru furnizarea serviciului de editare foto. Dacă utilizatorul nu poate folosi aplicația fără a fi de acord cu prelucrarea acestor date, consimțământul nu este acordat în mod liber”.



De reținut! Datele personale nu pot fi oferite drept plată pentru serviciile online gratuite.

Consimțământul se consideră a fi valabil numai dacă sunt puse la dispoziție servicii echivalente care nu depind de utilizarea datelor cu caracter personal, fără costuri suplimentare, subiectul având, astfel, libertatea de a alege. Echivalent, dacă persoana vizată decide să își retragă consimțământul, societatea nu are dreptul să solicite costuri suplimentare.

Pentru a fi liber, consimțământul trebuie acordat separat pentru fiecare scop specific al prelucrării.

b. Consimțământul trebuie să fie specific

Societatea care colectează datele (fie online, fie offline) trebuie să obțină consimțământul persoanei separat pentru fiecare activitate de prelucrare.

Pentru fiecare scop, trebuie furnizate informațiile specifice cu privire la datele prelucrate. Dacă se dorește utilizarea datelor colectate în scopuri noi, trebuie obținut un nou consimțământ înainte de a prelucra datele în noile scopuri.

! • **Exemplu de consimțământ specific:** În cazul în care la un târg (expoziție), o persoană își lasă datele pentru un concurs publicitar, societatea nu le va putea utiliza pentru a trimite ulterior mesaje de marketing.

! • **Exemplu oferit de Grupul de lucru „art. 29”:** „O rețea de televiziune prin cablu colectează datele personale ale abonaților, pe baza consimțământului acestora, pentru a le prezenta sugestii personalizate pentru filme. După un timp, rețeaua TV decide că ar dori să permită terților să trimită (sau să afișeze) publicitate vizată pe baza obiceiurilor de vizionare ale abonatului. Având în vedere acest nou scop, este necesar un nou consimțământ”.

c. Consimțământul trebuie să fie informat

Grupul de lucru „art. 29” furnizează o listă de elemente obligatorii care trebuie prezentate persoanei înainte de a i se cere consimțământul: identitatea fiecărui operator, scopul prelucrării, tipurile de date colectate, existența dreptului de retragere a consimțământului și, dacă e cazul, informații despre profilare sau decizii automate cu impact semnificativ și informații privind posibilele riscuri de transfer către state terțe UE.

Informarea trebuie să utilizeze un limbaj simplu și ușor de înțeles și trebuie să se diferențieze de termenii generali.

Dacă consimțământul este obținut prin semnare – pe un document/tabel etc., informarea trebuie să fie distinctă față de alte documente, astfel încât să nu se piardă printre alte informații.

Dacă discutăm de un consimțământ online, trebuie ca la loc vizibil să fie un buton/link către „Politica de confidențialitate” a societății, astfel încât persoanele să se poată informa în privința scopului, a posibilității de retragere a consimțământului etc.

d. Consimțământul trebuie să fie lipsit de ambiguitate

O non-acțiune, o lipsă a exprimării consimțământului expresă sau căsuțele pre-bifate nu valorează consimțământ.

Grupul de lucru „art. 29” recomandă operatorilor să facă uz de declarații scrise, însă, întrucât acest lucru nu este întotdeauna realist, se poate apela la alternative, precum declarații verbale înregistrate, răspunsuri la e-mail-uri și mesaje electronice, căsuțe cu posibilitate de bifare activă.

Grupul menționează că „GDPR pune la dispoziția controlorilor obligația de a dezvolta modalități de abordare a acestei probleme”.

● **Exemple de consimțământ ambiguu:**

• „În cazul în care nu veți bifa căsuța de mai jos, noi vom înțelege că dumneavoastră doriți să primiți newsletterele noastre”.

• Mulți operatori consideră faptul că dacă în cadrul unui newsletter există linkul de dezabonare, atunci consimțământul este reînnoit, ceea ce este greșit, acel link de dezabonare nereprezentând de fapt consimțământ.

Din experiența noastră, în rândul operatorilor se face o confuzie între menținerea și actualizarea/prelungirea consimțământului, iar, conform prevederilor GDPR, o astfel de practică reprezintă un mod de abordare greșit și un consimțământ nevalid.

O întrebare pe care o auzim destul de des se referă la consimțământul acordat înainte de 25 mai 2018. Continuă să fie valabil după această dată, când normele GDPR încep să fie aplicate?

În cazul în care consimțământul acordat de către o persoană anterior aplicării GDPR întrunește condițiile Regulamentului, nu este necesar ca societatea să solicite din nou consimțământul persoanelor fizice vizate.

● **Exemplu când nu este necesară obținerea unui consimțământ nou:** Pe site-ul unui organizator de evenimente exista și înainte de 25.05.2018 o căsuță prin care persoanele pot bifa dacă doresc să fie anunțate despre alte evenimente organizate de societatea respectivă. În Termenii și condițiile site-ului se puteau găsi toate informațiile necesare privind acel consimțământ (datele de identificare ale societății, pentru cât timp sunt reținute datele, cum se poate retrage consimțământul etc.). În acest caz, societatea nu va fi nevoită să solicite din nou consimțământul clienților.

● **Exemplu când este necesară obținerea unui consimțământ nou:** Un magazin online a obținut consimțământul clienților cu câțiva ani în urmă, folosind un sistem de căsuțe bifate în prealabil online. Este clar că acest mod de a obține consimțământul nu constituie un consimțământ liber exprimat începând cu data de 25 mai 2018, astfel încât societatea va trebui să obțină din nou consimțământul dacă dorește să prelucreză în continuare datele clienților săi.

Sub semnul întrebării stau și datele cu caracter personal făcute publice. Se pot transmite comunicări de marketing către aceste persoane?

Inițial trebuie identificat scopul pentru care aceste date au fost făcute publice (ex. un consultant își face cunoscută adresa de e-mail pentru a fi contactat pentru contractarea de servicii, o persoană alege să își creeze profil pe site-ul unei platforme de intermediere întâlniri (dating) pentru a primi e-mail-uri de la persoane interesate să cunoască oameni noi). În acest caz este evident că aceste persoane nu au dorit să primească oferte de pantofi de exemplu.

În ceea ce privește datele cu caracter personal care doar „plutesc” pe internet, fără posibilitatea de a stabili motivul pentru care persoana vizată și-a dezvăluit datele, răspunsul la întrebarea dacă sau nu să se trimită comunicări de marketing este evident – nu, deoarece prelucrarea nu va putea fi legitimată de către operator. Iar datorită GDPR, riscul unei interpretări extensive sau relaxate ar putea costa mai mult societatea decât veniturile pe care ar putea să le obțină din trimiterea unor oferte unor persoane care nu sunt interesate de produsele sau serviciile sale.

Pentru ce perioadă se acordă consimțământul?

În preambulul (39) al GDPR se vorbește despre „asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum”, precum și că „în vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică”.

Prin urmare, ori de câte ori se realizează o operațiune de prelucrare, trebuie menționată foarte clar perioada pentru care se vor stoca datele în cauză, iar aceasta perioadă nu trebuie să fie mai mare decât perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele.

Nu există un termen-limită al consimțământului. În general, odată ce acesta este valabil, el nu are termen de expirare și datele pot fi prelucrate până când persoana își va retrage consimțământul.

Cu toate acestea, dacă consimțământul a fost dat în scopul unei campanii care a avut o scurtă perioadă, acesta nu este suficient pentru campanii ulterioare, odată ce campania inițială a încetat. De exemplu, consimțământul dat pentru e-mail-uri privind un serviciu nou lansat, nu va fi valabil pentru alte servicii care vor fi lansate ulterior.

Din acest motiv este foarte important cum se formulează fraza prin care se acordă consimțământul.

! **Exemplu:** „sunt de acord să primesc noutăți despre organizarea de excursii în Italia” față de „sunt de acord să primesc noutăți despre orice excursii organizate de agenția de turism”.

De asemenea, dacă un client și-a dat consimțământul odată ce s-a abonat la un serviciu, consimțământul va expira atunci când acesta va renunța la acel serviciu. Organizația nu ar trebui să se bazeze pe consimțământ pentru a recăștiga clientul.

Retragerea consimțământului

Primul lucru important: Consimțământul este reversibil.

Art. 7 (3) din GDPR prevede: „Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia”.

Al doilea lucru important: GDPR obligă operatorii să se asigure că consimțământul poate fi retras la fel de ușor cum a fost dat.

Astfel, dacă pentru prelucrarea datelor în scop de marketing sau vânzări persoana și-a dat consimțământul prin apăsarea unui singur buton (click), ar trebui implementată o metodă la fel de ușoară pentru retragerea consimțământului.

Este bine ca în procedura de marketing să se stabilească modalitatea cea mai ușoară pentru persoanele care și-au dat consimțământul pentru a-l retrage. Cea mai uzitată este folosirea e-mail-ului (în acest mod se asigură și verificarea persoanei care solicită retragerea – dacă e-mailul este trimis de pe adresa de e-mail aflată în baza de date, se face automat și o verificare în acest sens) – ideal de folosit când consimțământul s-a trimis prin e-mail. Altfel, se mai folosește un formular online, dar care trebuie să conțină cât mai puține câmpuri.

! **Exemplu:** Nu se poate obține consimțământul printr-un simplu click, dar pentru retragere să se solicite o scrisoare trimisă prin poștă.

Al treilea lucru important: consimțământul trebuie să poată fi retras în orice moment și în mod gratuit, dar nu neapărat prin aceeași acțiune.

Astfel, un consimțământ privind primirea de noutăți privind organizarea de noi evenimente obținut prin semnarea olografă în cadrul unui târg, poate fi retras prin trimiterea unui email.

Al patrulea lucru important: Retragera consimțământului nu trebuie să aducă vreun inconvenient pentru persoana vizată (cum ar fi de exemplu pierderea garanției extinse pentru produsul achiziționat).

Neasigurarea unui mecanism de retragere duce la eșecul validității acordului.

Util de folosit: Acest lucru este esențial a fi prevăzut și în Procedura de Marketing a societății, fiind important a fi stabilit la acea procedură toți pașii care trebuie îndepliniți pentru a fi valabilă retragerea consimțământului (cine se ocupă din cadrul societății, când, cum etc. Procedura trebuie să prevadă ca datele să fie șterse din toate bazele de date, inclusiv din corespondența purtată. Dacă este vorba de un sistem automatizat trebuie verificat de asemenea cu atenție dacă acesta oprește prelucrarea datelor conform cerinței persoanei vizate).

În cazul retragerii, prelucrarea care a avut loc anterior rămâne legală, însă prelucrarea ulterioară trebuie să înceteze. Bineînțeles, nimic nu împiedică posibilitatea ca persoana vizată să își dea din nou consimțământul.

În cazul persoanelor vizate care au transmis către o societate date cu caracter personal, prin intermediul aplicațiilor de comunicare directă (de exemplu: messenger-ul de la Facebook), societatea se va asigura că datele respective vor fi șterse în momentul retragerii consimțământului de către persoana vizată.



Exemplu de amendă pentru nerespectarea retragerii consimțământului: A.N.S.P.D.C.P. – Autoritatea Națională de Supraveghere a demarat o investigație în urma căreia a aplicat sancțiunea cu amendă, ca urmare a unei petiții prin care se reclama faptul că operatorul Artmark Holding SRL a transmis petentului mesaje comerciale nesolicitate pe adresa de e-mail a acestuia fără consimțământul său. Deși petentul solicitase societății să îi fie șterse datele cu caracter personal din baza de date a operatorului întrucât fuseseră obținute fără acordul său, acesta a continuat să primească din partea Artmark Holding S.R.L. mesaje comerciale nesolicitate pe adresa sa de e-mail.)

Consimțământul copiilor

Copiii necesită o protecție sporită pentru utilizarea datelor lor personale în scopuri de marketing. Societățile nu trebuie să exploateze lipsa de înțelegere sau vulnerabilitatea lor.

Articolul 8 alin. (1) din Regulament prevede că, atunci când consimțământul copilului este necesar pentru oferirea de servicii ale societății informaționale în mod direct, prelucrarea este legală doar dacă copilul a împlinit în mod legal 16 ani.

În continuare, textul legal prevede: „Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului”.

GDPR nu definește noțiunea de „servicii ale societății informaționale” însă îndrumări în acest sens regăsim într-o lucrare a Grupului de Lucru art. 29 din Directiva 95/46/CE adoptat la data de 28 noiembrie 2017 și revizuit la data de 10 aprilie 2018. Interpretarea oferită de grupul de lucru are la bază jurisprudența Curții de Justiție a Uniunii Europene, ce a statuat că serviciile societății informaționale se referă la contracte și alte servicii care sunt încheiate și transmise online. În continuare, ghidul ne arată că în cazul în care un serviciu are două componente independente economic, una online – acceptarea ofertei în contextul încheierii unui contract sau activitățile de marketing și una fizică, de exemplu, livrarea efectivă a serviciului sau produsului, doar prima este inclusă în noțiunea de serviciu al societății informaționale, livrarea fizică a serviciului neintrând în aceeași categorie.

Pentru copiii sub vârsta de 16 ani, societățile trebuie să obțină consimțământul de la cei care au autoritatea părintească asupra acestora, cu excepția cazului în care serviciul pe care îl oferă este un serviciu online de prevenire sau consiliere dedicat copiilor.

O altă problemă ce se impune a fi pusă în discuție în contextul consimțământului copiilor este cea a oferirii în mod direct a serviciilor societății informaționale unui copil. Practic, dacă serviciile societății informaționale se adresează persoanelor ce au împlinit vârsta de 18 ani atunci serviciul nu va fi considerat ca fiind oferit în mod direct unui copil. Desigur, în aceste situații, operatorul trebuie să poată demonstra că persoanele vizate sunt cele ce au împlinit vârsta de 18 ani și că această condiție nu este doar o formalitate (așa cum arată Grupul de lucru art. 29, condiția nu ar trebui să fie compromisă, spre exemplu, de conținutul unei pagini de internet sau planurile de marketing, ce pot demonstra contrariul).

Ce înseamnă acest lucru? Dacă targetul societății îl reprezintă adolescenții (persoane sub 18 ani), dacă toate mesajele publicitare sunt îndreptate spre persoane minore, aceștia nu vor putea invoca ulterior că ei de fapt se adresau persoanelor majore.

Oferirea directă a serviciilor societății informaționale în baza consimțământului impune operatorilor de date efectuarea unor verificări în ceea ce privește îndeplinirea condiției vârstei de 16 ani pentru validitatea consimțământului digital.

Pentru verificare trebuie să fie avute în vedere două situații privind exprimarea consimțământului digital al copiilor: dacă utilizatorul afirmă că a împlinit vârsta minimă necesară, caz în care operatorul trebuie să efectueze verificări adecvate pentru a se asigura că această declarație este adevărată și dacă utilizatorul afirmă că nu a împlinit vârsta minimă pentru consimțământul digital, situație în care operatorul poate accepta acest răspuns, fără alte verificări. În plus, în efectuarea acestor verificări, operatorul trebuie să aibă în vedere să nu ajungă la o prelucrare excesivă a datelor personale, sens în care WP29 recomandă o evaluare a riscurilor pe care le implică prelucrarea datelor pentru verificarea validității consimțământului digital oferit de un copil.

În concluzie:

- Dacă persoana vizată are sub 16 ani, trebuie să existe consimțământul părintelui sau al tutorelui;
- Dacă persoana vizată are între 16 și 18 ani, prelucrarea datelor cu caracter personal ale unui copil este legală, dar societatea trebuie să efectueze verificări adecvate pentru a se asigura că această declarație este adevărată.

Dacă societatea poate verifica vârsta copilului respectiv (de exemplu, în cazul unei societăți care oferă cursuri de fotbal sau o școală de șah pentru copii), atunci este simplu – pentru noutăți trimise pe email se va cere consimțământul părintelui, dacă copilul are sub 16 ani sau adolescentului, dacă acesta are peste 16 ani.

Mai complicat este însă în situația în care se oferă servicii online, precum un serviciu pentru descărcarea muzicii, caz în care apare problema modului în care se poate verifica vârsta persoanei care vrea să fie ținută la curent cu noutățile care apar.

Cu privire la exprimarea acordului părintelui sau tutorelui, GDPR nu face referiri la metode practice de obținere sau de verificare a acestuia. Grupul de lucru arată că verificarea cu privire la persoana care își exprimă propriul consimțământ sau cu privire la persoana care exprimă consimțământul în numele copilului trebuie să se raporteze la riscurile specifice prelucrării și tehnologia utilizată.

Astfel, în situația în care riscurile prelucrării ar fi scăzute, verificarea răspunderii părintești ar putea fi efectuată doar prin intermediul unui e-mail. Însă, dacă riscurile prelucrării ar fi ridicate, operatorul de date poate apela la mai multe metode de verificare.



De reținut! De menționat este faptul că acordul pentru prelucrarea datelor oferit sau autorizat de titularul autorității părintești expiră odată ce minorul a atins vârsta minimă obligatorie pentru exprimarea consimțământului, ceea ce înseamnă că operatorul trebuie să obțină consimțământul de la persoana vizată ale cărei date personale fac obiectul prelucrării după ce aceasta a împlinit 16 ani.

Cu siguranță, verificarea consimțământului digital al copiilor reprezintă, pentru operatorii de date, o adevărată provocare în contextul GDPR. Aceștia vor fi nevoiți să identifice în ce măsură este necesar să implementeze sisteme sau proceduri pentru verificarea vârstei persoanelor a căror date sunt prelucrate nu doar la momentul colectării, ci și periodic, pentru a reaminti utilizatorilor că acordul exprimat sau autorizat de titularul răspunderii părintești expiră odată cu împlinirea vârstei de 16 ani, iar din acel moment, consimțământul trebuie reafirmat de către persoana vizată ale cărei date cu caracter personal se prelucrează.

Bune practici privind obținerea consimțământului

a. Cereți consimțământul pentru păstrarea adresei de e-mail și trimiterea de newslettere separat de aprobarea termenilor și condițiilor (T&C).

Majoritatea magazinelor online obișnuiau să solicite un singur acord și pentru Termeni și condiții și pentru trimiterea ulterioară de noutăți (newsletter) – sau pentru intrarea într-un club de cumpărători, acordul pentru transmiterea informațiilor către terți etc., explicația fiind că își doreau ca experiența pe care o aveau utilizatorii pe site-ul respectiv să fie cât mai plăcută, fără „plictiseala” de a citi prea mult sau a pierde timpul cu prea multe bife.

De asemenea, există teama că foarte puține persoane ar fi bifat și altceva ce nu era obligatoriu pentru a primi produsul de pe site.

b. Acordați o atenție deosebită bazei de date unde colectați informații despre consimțământ – „cine, când, cum?”

Potrivit art. 7 alin. (1) din Regulament, operatorul trebuie să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare a datelor cu caracter personal.

În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

GDPR nu numai că stabilește regulile privind modul de colectare a consimțământului, dar, de asemenea, impune societăților să țină o evidență a acestora.

Asta înseamnă că trebuie să puteți dovedi:

- Persoana care a consimțit;
- Când a consimțit;
- Ce informații a primit persoana respectivă în momentul consimțământului;
- Cum a consimțit (de exemplu, în timpul efectuării plății, prin formularul Facebook etc.);
- Dacă persoana și-a retras consimțământul;

Dovada luării consimțământului în format electronic va fi stocată în baza de date și după ce acesta va fi retras, până la respectarea obligațiilor legale, după caz, sau până la dispariția unui potențial litigiu între operator și persoana vizată.

Cel mai important de reținut este faptul că societatea trebuie să poată demonstra, la cererea autorității, faptul că bifele (care reprezintă consimțământul) se înregistrează în baza de date în mod legal și că se poate scoate un extras din această bază de date cu data și ora la care o anumită persoană și-a dat consimțământul.

c. Este recomandat să folosiți procesul de alegere dublă (cunoscut și ca alegere confirmată – double opt in).

Acest sistem presupune ca persoanele care și-au dat consimțământul pentru prelucrarea datelor în scop de marketing să confirme solicitarea făcând clic pe un link trimis la adresa lor înregistrată de e-mail. Acest sistem ajută societățile să se asigure că solicitarea este intenționată, nu a fost menționată de un terț și că adresa de e-mail furnizată este legitimă și funcțională.

Procesul de alegere dublă funcționează în modul următor:

- Persoana de contact nouă utilizează un formular de abonare sau o pagină de destinație pentru a se abona la un buletin informativ sau pentru a-și ajusta nivelul de consimțământ;
- După completarea cu adresa de e-mail, se afișează o pagină care menționează rugămintea de a-și verifica e-mailul pentru un mesaj de confirmare care include un link pe care persoana de contact trebuie să facă clic pentru a-și confirma solicitarea;

- Se trimite un e-mail de confirmare de tipul adecvat (abonare sau consimțământ) la adresa înregistrată pentru persoana de contact;
- Persoana de contact deschide e-mailul de confirmare, citește textul și face clic pe link. Acesta deschide un browser web, care remite un URL codat care identifică persoana de contact și mesajul de solicitare;
- Sistemul înregistrează clicul, aplică modificarea de abonament sau consimțământ, înregistrează modificarea și poate redirecționa către o pagină de mulțumire care este afișată persoanei de contact.

Acest sistem este recomandat a fi folosit mai ales pentru obținerea consimțământului unui copil (prelucrarea datelor acestuia) când este recomandabil să se solicite confirmarea de pe adresa de e-mail a părintelui.

d. Dacă există intenția de face un parteneriat privind baza de date obținută în temeiul consimțământului cu niște parteneri comerciali, trebuie să existe certitudinea că și aceștia au adoptat măsuri tehnice și organizatorice adecvate privind consimțământul și că, de asemenea, clienții ale căror date sunt preluate, acceptă acest transfer de informații.



• **Exemplu:** un salon de nunți și un organizator de evenimente decid să se promoveze împreună. Persoana vizată trebuie informată de faptul că datele (în acest caz adresa de e-mail sau telefonul, data nunții, calitatea – mire, mireasă, naș, socru) vor fi transferate și către partener. De asemenea, ambele societăți trebuie să aibă grijă ca politica de confidențialitate a celeilalte societăți să fie legală și bine implementată.

e. La momentul obținerii consimțământului, să vă asigurați că link-ul către politica de confidențialitate este vizibil și poate fi accesat cu ușurință. Vom detalia într-un subcapitol ce trebuie să conțină Politica de confidențialitate.

f. În cazul în care consimțământul se obține printr-un chestionar cu privire la alt subiect sau alt formular (cum ar fi un sondaj de opinie, formular de feedback etc.), solicitarea consimțământului trebuie să se facă printr-un câmp separat (clar delimitat de alte întrebări din formular) și să furnizeze informațiile esențiale legate de consimțământ.

g. În colectarea datelor personale despre copii, societatea trebuie să se asigure că se fac toate eforturile să se informeze corect copilul sau părintele despre scopul prelucrării datelor personale ale copilului.

În cazul în care se utilizează materiale promoționale adresate direct copiilor sau se colectează date de la ei cu acest scop, informațiile trebuie să fie vizibile, ușor de citit și înțeles de către copii.

În toate cazurile în care este necesar un consimțământ expres, operatorul trebuie să obțină consimțământul expres al părintelui. Societatea trebuie să adopte măsuri rezonabile pentru verificarea faptului că persoana care exercită drepturile copilului este părintele acestuia (cum ar fi metoda double opt in).

h. Este bine ca în Politica de confidențialitate prezentată pe site-ul societății să existe un capitol distinct, ușor de identificat, privind retragerea consimțământului. Este important ca orice persoană să poată înțelege cum trebuie să procedeze pentru a-și manifesta voința în sensul retragerii consimțământului.

Prelucrarea se bazează pe un interes legitim

Deși cel mai des este folosit consimțământul ca temei al prelucrării de către departamentele de Marketing și Vânzări, nu este de neglijat nici interesul legitim. În acest caz nu se mai pune problema colectării acordului persoanei pentru a-i fi prelucrate datele cu caracter personal, nici problema dovedirii obținerii acestor acorduri (însemnând costuri reduse pentru Societate), fiind vorba doar de informarea corectă și completă a persoanelor.

GDPR:

„(47) Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia”.

Principiul transparenței: se va avea în vedere o comunicare transparentă în relația cu persoana vizată. Informațiile vor fi ușor accesibile și ușor de înțeles (limbaj simplu și clar).

Existența unui interes legitim necesită o evaluare a riscurilor (studiu de impact). Prin acest studiu de impact, societatea trebuie să analizeze dacă:

a. Persoana vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal posibilitatea prelucrării în acest scop;

b. Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date.

Un interes legitim trebuie să fie „acceptabil în condițiile legii”:

- să fie legal (în conformitate cu cerințele naționale și UE),
- să fie suficient de clar pentru a permite efectuarea testului de proporționalitate în raport cu drepturile și interesele persoanelor vizate,
- să reprezinte un interes real și prezent (să nu fie speculativ).

În cazul în care compania ia în calcul să își întemeieze colectarea și prelucrarea pe interes legitim (și să nu solicite consimțământ de la persoanele vizate), este indicat să desfășoare o evaluare de impact privind interesul legitim.

Factori cheie de avut în vedere în cazul evaluării de impact:

- a. Natura și sursa interesului legitim;
- b. Impactul asupra persoanelor vizate;
- c. Garanții pentru persoanele vizate.

Evaluarea de impact privind protecția datelor (DPIA – Data Protection Impact Assessment, sub denumirea care se regăsește în Regulament), se recomandă să fie realizată înaintea începerii prelucrării datelor cu caracter personal, să fie revizuită periodic (Grupul de lucru „art. 29” recomandă revizuirea DPIA la 3 ani sau mai puțin), în special dacă apar modificări cu privire la riscuri sau condiții.

Vom detalia această „evaluare de impact” în capitolul privind Prozedurile, acum ne vom referi doar la DPIA în domeniul Marketingului.

Astfel, în conformitate cu prevederile GDPR și potrivit recomandărilor formulate de Autoritatea de supraveghere britanică, coroborat cu precizările Autorității noastre naționale în domeniu (A.N.S.P.D.C.P.) care a emis o decizie în acest sens – Decizia nr. 174/2018 (ce reglementează situațiile când trebuie realizată DPIA) și precizările Grupului de lucru „art. 29” (WP248), cu privire la efectuarea unei evaluări DPIA, vă menționăm câteva lucruri de care trebuie să aveți grijă atunci când efectuați un studiu de impact:

- Analizarea și identificarea necesității realizării evaluării DPIA: când societatea dorește să prelucreze date cu caracter personal în scop de marketing fără a solicita consimțământul persoanelor vizate;

- Se va descrie prelucrarea: este importantă o detaliere a tipului de prelucrare (dacă aceasta se va realiza online, se vor indica exact butoanele și link-urile folosite – eventual se va include o anexă cu o fotografie a interfeței);

- Se ia în calcul consultarea Autorității de supraveghere;

- Se analizează necesitatea și proporționalitatea (tot timpul în acest domeniu se verifică proporționalitatea dintre drepturile operatorului – a societății care dorește să prelucreză în scop de marketing date cu caracter personal fără a obține consimțământul persoanei vizate și drepturile persoanei vizate);
- Se identifică și evaluează riscurile apărute (bineînțeles, ne referim la riscurile apărute atât pentru persoana vizată care nu și-a dat consimțământul expres dar și pentru societate);
- Se identifică măsuri tehnice și organizatorice care limitează riscurile (este bine ca lista măsurilor să fie detaliat descrisă și apoi implementată, astfel încât să nu fie doar de formă menționată în DPIA);
- Se vor integra rezultatele în procedurile de conformare la GDPR (acest DPIA trebuie văzut ca parte integrantă în procedura referitoare la departamentul de marketing al societății);

Este recomandat a se relua permanent argumentele din DPIA, pentru a analiza dacă apar modificări în procesarea dorită din perspectiva rezultatului acesteia.

O evaluare a impactului poate reduce anumite costuri în desfășurarea activității unei companii (de exemplu, în urma evaluării se poate decide că într-un anumit caz nu mai trebuie obținut consimțământul persoanelor vizate, însemnând astfel costuri mai mici pentru societate) și are ca rol minimizarea riscurilor în ceea ce privește prelucrarea datelor cu caracter personal.

Activități specifice Departamentului de Marketing în contextul GDPR

Site-ul societății. Bune Practici

Site-ul societății nu reprezintă doar o metodă facilă de prezentare a activității acesteia (detaliindu-se produsele și serviciile), ci și un loc unde societatea își publică politicile (Termeni și Condiții, Politica de Confidențialitate sau Politica de cookie-uri). Este locul pe care diferite autorități ale statului verifică conformitatea societății la obligațiile legale ale acesteia – site-urile fiind vizitate nu doar de către ANPC, ci și de Ministerul de Finanțe, Consiliul Concurenței sau A.N.S.P.D.C.P.

Societățile trebuie astfel să acorde o atenție sporită site-ului, nu doar din punct de vedere estetic și al atractivității către consumator, ci și din punct de vedere legal.

Bune practici privind site-ul societăților:

a. În cazul multor site-uri, există un formular de contact astfel încât o persoană interesată să poată trimite direct ce întrebări are fără a mai ieși de pe respectiva pagină pentru a trimite un e-mail. De foarte multe ori pe pagina de contact se solicită prea multe informații, încălcându-se astfel principiul minimizării datelor.



• **Exemplu:** se solicită ocupația părintelui (a celui care dorește să intre în contact cu site-ul) pe un site ce oferă informații despre organizarea de tabere pentru copii sau se solicită vârsta pe un site de consultanță de mediu. În acest caz, maximul ar fi trebuit să fie o simplă bifă că persoana are peste 18 ani.

b. Un alt lucru care trebuie avut în vedere în ceea ce privește datele cu caracter personal și site-ul societății, este acela că pe pagina de contact este uzual să se pună o hartă cu locul unde se află sediul societății care administrează respectivul site.

De cele mai multe ori, nu este vorba de o simplă fotografie, ci este integrată o hartă Google.

Trebuie avut în vedere faptul că serviciul de cartografiere Google Maps ar putea colecta, prelucra și exploata datele persoanelor în mod automat, chiar fără ca acestea să intre pe respectiva hartă și atunci ar trebui informate și persoanele care accesează respectivul site.

c. Este recomandat ca incorporarea videoclipurilor de pe YouTube să se realizeze cu opțiunea activată pentru setările avansate de confidențialitate a datelor. Dacă o persoană redă (vizionează) aceste videoclipuri, cookie-urile YouTube și cookie-urile DoubleClick sunt stocate pe computerul respectiv și datele vor fi transmise către Google Inc., în calitate de operator al YouTube.

La redarea videoclipurilor stocate de YouTube, conform informațiilor curente, vor fi transmise către Google Inc., în calitate de operator al YouTube și al rețelei DoubleClick, cel puțin următoarele date: adresa IP și ID-ul cookie-ului, adresa specifică a paginii accesate, data și ora de acces a sistemului, ID-ul browser-ului. Transmiterea acestor date se efectuează independent dacă persoana are un cont de utilizator Google prin care este conectat sau nu are un cont de utilizator.

YouTube sau Google Inc. stochează astfel de date ca profiluri de utilizare și, dacă este cazul, le utilizează în scopuri de marketing, de cercetare de piață și/sau de proiectare bazată pe cerere de site-uri de internet. O astfel de analiză este efectuată în special (și pentru utilizatorii

care nu sunt conectați), pentru a oferi publicitate bazată pe cerere și pentru a informa alți utilizatori despre activitățile efectuate de pe anumite site-uri.

Bineînțeles că persoanele au dreptul să se opună față de crearea unor astfel de profile de utilizatori contactând Google în calitate de operator al YouTube, dar puțini o fac – fie din neștiință, fie că li se pare foarte complicat.

d. Securitatea este un pas extrem de important. Un prim pas pentru securizarea site-ului ar fi adăugarea unui certificat SSL website-ului în cazul site-urilor în Wordpress (vom detalia acest aspect în Capitolul privind măsurile tehnice și organizatorice).

e. Dacă o societate dă posibilitatea ca pe site să se poată comenta la diferite articole/prezentări/informări, atunci trebuie avută grijă și de acele căsuțe – persoanele să fie informate asupra drepturilor lor și de asemenea, să se dea posibilitatea ca respectivele persoane să poată solicita retragerea consimțământului.

f. Adresele IP sunt considerate date cu caracter personal, deoarece se poate identifica locația exactă a unui utilizator. Dat fiind faptul că acestea sunt colectate imediat ce script-urile Google Analytics și Google Tag Manager rulează, adică imediat ce o persoană accesează un website, utilizatorul nu are timp să își dea consimțământul. Astfel, societățile vor fi nevoite să anonimizeze aceste adrese IP. Acest lucru se poate face direct din Google Tag Manager.

De asemenea, este recomandată instalarea unui Firewall website și instalarea unui soft pentru detectarea în timp real a fișierelor malițioase.

g. Trebuie acordată o atenție sporită și informațiilor primite pe chat, dacă societatea a implementat un asemenea instrument. Pe lângă IP-ul colectat automat (a se vedea punctul f de mai sus), persoanele își pot lăsa foarte multe date personale acolo (exemplu: „Mă interesează să achiziționez un telefon pentru copilul meu de 10 ani. Noi stăm în Vadu Morii și venim rareori la București. Mă interesează un telefon ieftin, veniturile mele sunt mici și sunt și divorțată...”).

În Politica de confidențialitate trebuie prevăzute proceduri și pentru informațiile lăsate acolo de persoanele care doresc să intre în contact cu un reprezentant al societății, cât vor fi stocate, cine va avea acces la ele etc.

h. În cazul în care este numit un DPO, acesta va trebui să discute periodic cu reprezentanții Departamentului de Marketing sau cu societatea împuternicită să se ocupe de site-ul societății pentru a fi la curent cu ce modificări se intenționează a se aduce site-ului. În cazul în care societatea nu are numit un responsabil de date cu caracter personal, este bine ca o

persoană din cadrul Departamentului de Marketing să aibă ca responsabilitate (inclusiv menționată în fișa postului) de a verifica site-ul periodic din punct de vedere al conformării la normele GDPR.

Politica de confidențialitate

Unul dintre principiile fundamentale pe care GDPR îl impune a fi respectat în cadrul oricărei operațiuni de prelucrare a datelor cu caracter personal este principiul transparenței, menționat în mod expres la art. 5 alin. (1) din GDPR: „(1) Datele cu caracter personal sunt: a) prelucrate în mod legal, echitabil și transparent față de persoana vizată («legalitate, echitate și transparență»)”.

Trebuie menționat faptul că principiul transparenței reglementează în special relația dintre societate și persoana vizată. Conform acestui principiu, operațiunile de prelucrare trebuie să fie explicate persoanelor vizate într-un mod ușor accesibil, care să garanteze că acestea înțeleg ce se întâmplă cu datele lor cu caracter personal.

Se impune informarea persoanei vizate asupra:

- identității operatorului și a reprezentantului acestuia, dacă este cazul (am văzut mai multe site-uri unde nu era menționat ce societate administrează site-ul respectiv, bineînțeles cu toate datele de identificare; sau în cazul unui târg se solicită adresa de e-mail pentru a fi informată de existența altor evenimente, dar se comunică cine exact este organizatorul);
- scopurile în care sunt prelucrate datele cu caracter personal (statistică, publicitate etc.);
- temeiul juridic al prelucrării datelor (consimțământ, interes legitim etc.);
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal (la cine vor ajunge datele – în exemplul dat mai sus cu salonul de nunți și organizatorul de nunți, trebuie informate persoanele fizice că datele vor ajunge și la partenerul societății care colectează datele);
- asupra existenței drepturilor aparținând persoanei vizate cu privire la datele sale personale;
- datele de contact ale responsabilului cu protecția datelor (dacă acesta există, dacă nu este recomandat să existe măcar o adresă de e-mail dedicată);
- dacă este cazul, intenția societății de a transfera date cu caracter personal către o țară terță sau o organizație internațională;

- perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

- atunci când prelucrarea se bazează pe consimțământul persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

- dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;

- în cazul existenței unui proces decizional automatizat incluzând crearea de profiluri, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată;

- în cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv;

- aspecte suplimentare privind obligația de informare se adaugă în sarcina operatorului, în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată. Este notabilă obligația de informare privind sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public, ce reprezintă, desigur, o concretizare a principiului transparenței.

Recomandarea Grupului de Lucru art. 29 este ca orice informare în format electronic să fie realizată în mod diferențiat/fragmentat/punctual (noțiunea oficială în limba engleză fiind „layered privacy statement”), astfel încât persoana vizată să poată accesa cât mai clar, în mod distinctiv, orice porțiune de informație va considera a fi relevantă. Alte mijloace electronice de informare pot include pop-up-urile contextuale care apar chiar înainte ca persoana vizată să ofere datele personale, imaginile 3D sau notificările ce se suprapun paginii principale. Alte mijloace electronice grafice pot fi alăturate notificărilor scrise punctuale, incluzând aici alerte video sau audio. „Alte mijloace” pot include animații sau infografice.

Societățile, în general, colaborează cu avocați pentru redactarea Politicii de confidențialitate, ceea ce este excelent întrucât aceștia vor verifica ca toate informațiile obligatorii să fie conținute în cadrul acesteia,

dar nu înseamnă că odată redactată și postată, se termină răspunderea societății.

Politica de confidențialitate trebuie implementată prin măsuri tehnice și organizatorice și de asemenea, trebuie revăzută și revizuită periodic.

Cookie-uri. Politica de cookies a site-ului companiei

Majoritatea site-urilor colectează, prin intermediul cookie-urilor, date personale despre utilizatorii site-urilor. Aceste cookie-uri sunt de mai multe tipuri: esențiale (fără de care site-ul nu poate funcționa), de analiză, de preferințe, de marketing etc.

Există numeroase discuții privind intruziunea cookie-urilor asupra datelor persoanelor care intră pe un site, o parte finalizându-se cu opinii obligatorii ale CJUE cum ar fi cea din cauza C-673/17 din 01.10.2019 prin care s-a statuat faptul că utilizarea cookie-urilor trebuie să se facă în urma acordului activ al utilizatorilor, acord care se dă prin intermediul barei de cookie (banner de cookie).

Se recomandă ca un site să conțină:

- a. o notificare imediat vizibilă care informează dacă sunt utilizate diferite tipuri de cookie-uri, furnizând informațiile într-o așa-numită „abordare stratificată” (cookie-uri necesare, de profilare etc.);
- b. o notificare imediat vizibilă care informează că, utilizând site-ul web, utilizatorul înțelege că cookie-urile necesare vor fi plasate;
- c. informații care explică modul în care utilizatorul își poate exprima și reține ulterior consimțământul pentru cookies;
- d. un mecanism prin care utilizatorul să poată alege să accepte toate cookie-urile sau doar anumite cookie-uri sau să refuze plasarea acestora;
- e. o opțiune pentru ca utilizatorul să schimbe ulterior o preferință cu privire la cookie-uri.

Comportament activ:

Consimțământul pentru acceptarea unui anumit tip de cookie ar trebui să rezulte dintr-o acțiune pozitivă sau un alt comportament activ al utilizatorilor, cu condiția să fie informați despre consecințele acțiunii sau comportamentului lor.

Utilizatorii își pot exprima consimțământul:

- a. făcând click pe un buton sau pe un link;
- b. bifând o casetă în spațiul în care sunt prezentate informații despre utilizarea cookie-urilor;
- c. orice alt comportament activ din care operatorul poate concluziona că există un consimțământ expres al utilizatorului.

În vederea funcționării corespunzătoare, website-urile folosesc module cookies care întreprind diferite funcții dintre care: necesare, statistice sau de marketing. Cookie-urile sunt create pentru a permite website-ului să își recunoască utilizatorii și vizitele subsecvente sau să autorizeze alte website-uri să recunoască acești utilizatori.

Bara de cookie

Bara de cookie (bannerul de cookie) este mesajul (pop up) care se deschide la accesarea unei pagini de internet. Aceasta trebuie să conțină toate tipurile de cookie-uri folosite pe respectivul site urmate de căsuțe pe care persoana care intră pe respectivul site să le poată bifa (este important ca aceste căsuțe să nu fie prebifate sau să nu fie condiționată intrarea pe site de bifarea tuturor căsuțelor). Singura categorie de căsuță care poate fi prebifată este cea a cookie-urilor esențiale, fără de care site-ul nu poate funcționa.

Politica de cookies

Politica trebuie să fie afișată la loc vizibil pe site-ul societății. De asemenea, trebuie să existe un link către această politică la momentul la care persoana bifează căsuțele, astfel încât să fie informată despre ce cookie-uri sunt folosite, ce înseamnă fiecare cookie, unde vor fi transmise datele stocate de modulele cookie, precum și durata de stocare a datelor de către modulele cookie etc.

Recomandăm ca în cadrul acestei politici să se dea posibilitatea persoanelor care accesează site-ul să își poată modifica în orice moment opțiunile cu privire la cookie-uri.

Prin intermediul cookie-urilor de marketing, societatea va putea să îi urmărească pe utilizatori de la un website la altul cu intenția de a plasa anunțuri relevante și antrenante pentru utilizatori, să colecteze date cu privire la link-urile accesate de utilizatori, durata de navigare pe website, precum și termenii de căutare prin care au ajuns să navigheze pe website-ul societății (informație importantă pentru departamentul de Marketing).

Utilizatorii își vor da consimțământul cu privire la utilizarea modulelor cookies de marketing în momentul incipient al accesării website-ului prin bifarea căsuțelor corespunzătoare (opt-in).

Bifarea/debifarea semnifică un consimțământ valid de acceptare/retragere a consimțământului privind prelucrarea datelor cu caracter personal prin intermediul modulelor cookies pentru scopurile respective.

Persoanele însărcinate – salariați/mandatari din cadrul societății trebuie să asigure asistența utilizatorilor în cazul în care vor întâmpina dificultăți privind retragerea consimțământului cu privire la cookie-urile de marketing, în special, și cu privire la celelalte module cookies, în general, în cazul în care explicațiile prevăzute în politica cookies nu sunt inteligibile pentru utilizatori.

Instrumentele de consimțământ pentru cookie-uri pot include ecrane splash, bannere sau căsuțe de dialog modale.

Setările browser-ului pot exprima consimțământul utilizatorilor numai în circumstanțe limitate (în cazul în care operatorul poate demonstra că utilizatorul a fost informat în totalitate și i-a configurat activ browser-ul).

Site-urile web nu ar trebui să condiționeze accesul general la site-ul lor de acceptarea tuturor cookie-urilor.

Utilizatorilor ar trebui să li se ofere o alegere reală în ceea ce privește cookie-urile care nu sunt necesare în legătură cu scopul furnizării serviciului site-ului.

Neacceptarea cookie-urilor nefuncționale nu ar trebui să împiedice un utilizator să cumpere produse de pe site-ul respectiv.

Se recomandă ca terminalul și software-ul să ofere by default setări de protecție privind viața privată – privacy protective settings și să ofere opțiuni clare utilizatorilor pentru a confirma/schimba elementele setărilor.

Un cookie utilizat fără consimțământ ar trebui să aibă o durată de viață raportată la scopul pentru care este folosit site-ul/aplicația și ar trebui să expire când nu mai este necesar, ținând cont de așteptările rezonabile ale utilizatorului/abonatului. Astfel, cookie-ul ar trebui să expire la momentul închiderii sesiunii sau chiar mai devreme.

De analizat: cazul coșului de cumpărături – operatorul poate seta cookie-ul să persiste după închiderea sesiunii pentru câteva ore/zile etc. (utilizatorul închide sesiunea și ar putea avea așteptarea rezonabilă ca la momentul revenirii să își recupereze conținutul coșului de cumpărături) – interes legitim.

Sau ar trebui să solicite consimțământul persoanei vizate pentru a reține informații de la o sesiune la alta?

Analiza site-ului cu Google Analytics

Majoritatea site-urilor utilizează serviciul „Google Analytics” furnizat de Google Inc. pentru a analiza modul de utilizare a site-ului de către utilizatori. Informațiile colectate prin intermediul cookie-uri-lor sunt în general transmise către un server al Google din SUA și stocate acolo. În conformitate cu acordul de prelucrare a datelor încheiat de operatorii

site-urilor de internet cu Google Inc., Google Inc. compilează o analiză a utilizării site-ului și a activității site-ului prin intermediul datelor colectate și oferă servicii legate de utilizarea internetului.

Informațiile culese de la aceste cookie-uri – de exemplu, ora, locul și frecvența utilizării website-ului de către utilizatori sunt, de obicei, transmise către un server Google din SUA și stocate acolo. Utilizarea clasică a Google Analytics nu exclude alte date personale în plus de adresa IP care este capturată de cookie-urile Google Analytics.

Recomandăm astfel ca anonimizarea IP să fie activă pe site-uri (se anonimizează de fapt ultima cifră din IP). Scurtarea adreselor IP asigură că nu poate fi stabilită nicio conexiune către un vizitator individual al website-ului.

Persoanele au opțiunea de a preveni stocarea cookie-urilor pe dispozitive (inclusiv pe laptop sau telefoane) prin efectuarea modificărilor corespunzătoare în setările browser-ului. Utilizatorii pot, de asemenea, preveni datele produse de cookie-uri și cu privire la capturarea utilizării website-ului de către aceștia (inclusiv adresele lor de IP) și procesării de către Google prin descărcarea și instalarea unor inserturi în browser, disponibile prin link-ul de mai jos. Adresa curentă de legătură este: <https://tools.google.com/dlpage/gaoptout?hl=en>.

Profilarea, un instrument de marketing din ce în ce mai des folosit de către companii

Majoritatea companiilor impun un ritm de creștere anuală (a cifrei de afaceri sau a profitului). Cum nu se mai vorbește de satisfacerea nevoilor de bază pe teritoriul Uniunii Europene, această creștere se poate realiza până la un anumit prag, după care cerința de produse sau servicii noi va trebui stimulată pentru a mai putea crește. Stimularea, datorită dezvoltării tehnologice, se poate realiza acum, la nivel de nevoi individuale, în funcție de preferințele și comportamentul fiecărui utilizator de internet în parte. Companiile exploatează aceste nevoi ajungând astfel mult mai ușor la comportamentul și opiniile personale ale consumatorilor, trimițându-le oferte pe măsura tipologiei personale ale acestora. Le este mai ușor să înțeleagă motivația deciziilor de a cumpăra ceva.

Nu este în sine un lucru rău – o femeie care de abia a născut ar putea fi interesată să primească oferte de botoșei de exemplu în locul unei oferte de bocanci bărbățești pentru hiking sau o persoană care practică înotul

poate ar prefera să primească noutăți și informații despre acest sport decât despre unelte de grădinarit dacă nu are și acest hobby, bineînțeles.

Problema vine atunci când comportamentul unui consumator este utilizat în scopuri ilegale (de exemplu, pentru a-i influența decizia de vot) sau fără acordul acestuia. Sunt nenumărate studii privind influența votului folosind profilarea și este bine să citim despre asta pentru a fi în cunoștință de cauză. În acest subcapitol discutăm despre profilarea în scop de marketing și vânzări, astfel încât nu vom atinge partea ilegală a identificării comportamentului unei persoane.

Crearea de profiluri și procesul decizional individual automatizat sunt utilizate pe scară largă în domenii precum cel bancar, financiar, sănătate, asigurări, marketing și publicitate. Dezvoltarea tehnologiei și creșterea capacităților de analiză a volumelor mari de date precum și inteligența artificială au determinat o diversificare și răspândire a acestor practici pe de o parte, dar și o amenințare la drepturile și libertățile persoanelor a căror date sunt prelucrate pe cealaltă parte.

În acest sens, Uniunea Europeană a simțit necesitatea introducerii unor noi reglementări care să protejeze drepturile și libertățile persoanelor vizate. Regulamentul General Privind Protecția Datelor introduce obligații de care companiile vor trebui să țină seama atunci când se folosesc de crearea de profiluri și procese decizionale individuale automatizate, în strategiile de business:

- cerințe specifice privind transparența și echitatea;
- responsabilitate sporită a operatorilor;
- temeuri juridice specifice privind prelucrarea datelor;
- informarea privind drepturile persoanelor vizate de a se supune creării de profiluri și, în mod expres, creării de profiluri în scop de marketing;
- în anumite situații, obligativitatea de a efectua o evaluare de impact asupra protecției datelor (DPIA).

Reglementările nu vizează doar deciziile luate ca urmare a prelucrării automate sau a creării de profiluri, ci și colectarea datelor în vederea creării de profiluri, precum și aplicarea respectivelor profiluri persoanelor.

Conform definiției, crearea de profiluri este un proces format din 3 elemente:

1. trebuie să fie o formă de prelucrare automată (folosindu-se inteligența artificială);
2. trebuie să fie efectuată asupra datelor cu caracter personal ale mai multor persoane;
3. obiectivul creării de profiluri trebuie să fie acela de a evalua aspecte personale în legătură cu o persoană fizică. Evaluarea

caracteristicilor sau a tipurilor de comportamente ale unei persoane permit încadrarea acesteia într-o anumită categorie sau un anumit grup, informații necesare pentru a plasa oferte comerciale specifice, în special pentru a analiza și/sau pentru a formula previziuni cu privire la:

- preferințele personale, interesele personale (cum am precizat mai sus, exemplu: hobby-uri, preocupări);
- comportamentul personal (stilul de viață, când preferă să cumpere anumite lucruri);
- situația economică (de mare interes pentru departamentele de Marketing și vânzări, pentru a ști ce ofertă se poate trimite);
- locurile în care se află persoana fizică respectivă;
- deplasările acestuia.



De reținut! Profilarea se va baza întotdeauna pe consimțământ expres.

Pentru ca operatorii să asigure conformitatea cu Regulamentul Privind Protecția Datelor, trebuie să țină seama de următoarele aspecte:

- Prelucrarea Datelor să fie legală, echitabilă, transparentă. Aceasta înseamnă că, pe lângă o prelucrare legală și echitabilă, operatorul trebuie să transmită persoanelor vizate informații concise, clare, ușor accesibile, inteligibile despre prelucrarea datelor lor cu caracter personal.

- Prelucrarea trebuie să fie limitată la scop. Crearea de profiluri poate presupune utilizarea unor date care au fost colectate inițial în alt scop, doar dacă scopurile sunt compatibile.

- Reducerea la minimum a datelor, chiar dacă operatorii sunt tentați să obțină mai multe informații despre persoanele vizate, în eventualitatea în care ar putea folosi aceste date cu alte scopuri.

- Datele colectate în vederea profilării trebuie să fie exacte și stocarea lor trebuie să fie limitată în timp.

- Să se respecte condițiile de integritate și confidențialitate de prelucrare a datelor, așa cum sunt ele descrise în GDPR: „protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.”

Operatorul trebuie să fie responsabil și mai ales, să poată dovedi în orice moment faptul că prelucrează datele respectând principiile mai sus menționate.

Astfel de prelucrări constând în activități decizionale individuale automatizate sau activități de creare de profiluri, în scop de marketing, pot fi realizate doar dacă:

- operatorul a informat persoana vizată și
- doar cu consimțământul persoanei vizate.



De reținut! În cazul în care o societate decide că este util să înceapă să își profileze clienții, va trebui să își numească un Responsabil de date cu caracter personal (DPO).

În acest sens, pe pagina sa, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal a specificat cazurile în care este obligatorie desemnarea unui responsabil cu protecția datelor, precizând de asemenea ce ar trebui să înțelegem prin expresia: „Monitorizarea periodică și sistematică” – ca reprezentând toate formele de urmărire și profilare pe Internet, inclusiv în scop de publicitate comportamentală, nefiind însă restricționată în mediul online.

„Exemple de situații care pot constitui o monitorizare periodică și sistematică a persoanelor vizate:

- gestionarea unei rețele de telecomunicații;
- profilare și scoring în scopul evaluării riscurilor (de exemplu, în scopul acordării unui credit, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor);
- urmărirea locației, spre exemplu prin aplicații mobile (geolocalizare);
- desfășurarea de programe de loialitate;
- monitorizarea stării de sănătate prin intermediul dispozitivelor portabile;
- televiziune cu circuit închis – CCTV;
- prelucrarea datelor pacienților de către un spital;
- prelucrarea datelor de conținut, locație, trafic de către furnizorii de servicii de internet;
- prelucrarea datelor personale de către companii de asigurări;
- publicitate comportamentală”.



De reținut! Atunci când o societate emite carduri de loialitate, deschide un „club” al celor care preferă un anumit brand etc., înseamnă că începe să își monitorizeze clienții, creându-le profiluri.

Este foarte important, de asemenea, ca atunci când o societate recurge la profilare, să precizeze acest aspect, fie în pagina dedicată

protecției datelor cu caracter personal de pe site, fie în Politica de confidențialitate.

Nu este suficientă „anunțarea” consumatorilor despre faptul că societatea creează profiluri, ci trebuie detaliat ce înseamnă profilarea în concret (profilare consumatorilor unui magazine online de pantofi este diferită de profilarea pe care o face un spital sau o agenție de turism de exemplu), mecanismul de profilare și scopul profilării.

În general, trebuie să evitați crearea de profiluri copiilor în scopuri de marketing. Trebuie, de asemenea, să respectați dreptul absolut al copiilor de a se opune profilării, care este legată de marketingul direct și să nu mai faceți acest lucru dacă vi se cere.

GDPR afirmă că nu trebuie să supuneți copiii deciziilor bazate exclusiv pe prelucrarea automată (inclusiv profilarea), în cazul în care acestea produc efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. Deși există excepții de la această interdicție, acestea se aplică numai dacă există măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale copilului, iar preambulul 71 al GDPR oferă o indicație clară că acestea nu ar trebui să fie regula. Deci, dacă luați în prezent aceste tipuri de decizii cu privire la copii, trebuie să examinați cu atenție această prelucrare.

Organizarea de concursuri și campanii promoționale

Concursurile sau campaniile promoționale nu pot fi organizate legal în România fără un Regulament Oficial al Concursului/Campaniei conform Ordonanței nr. 99 din 29 august 2000 privind comercializarea produselor și serviciilor de piață modificate. Acest Regulamentul Oficial de Concurs/Campanie va cuprinde și un capitol distinct denumit „Protecția datelor cu caracter personal”, un capitol foarte important de altfel.

Datele cu caracter personal oferite în mod voluntar de către participanți și obținute în cadrul concursului vor fi colectate de către Organizator, singur sau prin împuterniciii săi, diferite agenții/societăți cu activitate specifică care vor colecta datele participanților cu respectarea instrucțiunilor societății inserate fie în contractul de furnizare servicii, fie în acorduri separate de prelucrare de date.

Datele nu ar trebui să fie dezvăluite către terți, cu excepția salariaților autorizați/mandatarilor, împuterniciților acestora cărora aceste date le sunt necesare pentru a le prelucra în numele Organizatorului și partenerilor contractuali ai acestuia cărora aceste date le sunt necesare în vederea

desfășurării relației contractuale și a cazurilor în care se impune ca Organizatorul să respecte obligațiile impuse de legislația în vigoare sau în cazul în care participanții sunt informați în acest sens.

Datele cu caracter personal, oferite în mod voluntar de către participanți în cadrul Concursului/ Campaniei, vor fi păstrate, de regulă, până la livrarea premiului către câștigătorul desemnat, după care vor fi șterse, în măsura în care nu există alte obligații legale privind păstrarea acestora (de exemplu, pentru premiile a căror valoare depășește 600 RON când se vor păstra datele câștigătorilor în temei legal – declarare din punct de fiscal-contabil).

Este important ca angajații care se ocupă de organizarea de campanii publicitare să aibă trecute în fișa postului atribuții referitoare la prelucrarea datelor cu caracter personal și de asemenea, să fie instruiți în acest sens.

Trebuie avută o grijă deosebită în ceea ce privește colectarea datelor cu caracter personal pentru desfășurarea de concursuri – companiile nu vor putea utiliza bazele de date cu participanții colectate în mediul offline pentru campanii online decât dacă vor avea acordul explicit al persoanelor respective și nici folosirea datelor colectate în scop de concurs în alte scopuri.

În ceea ce privește concursurile organizate pe Facebook, acestea au un regulament strict, actualizat în permanență (ultima actualizare a avut loc pe 23 aprilie 2019). Astfel, societățile trebuie să includă Regulamentul concursului și condițiile de participare (și restricțiile de vârstă, restricțiile teritoriale etc.).

Dar trebuie să includă și faptul că nu Facebook/Instagram este responsabil de concurs, nefiind responsabil nici de colectarea și nici de prelucrarea datelor cu caracter personal.



● **Exemplu:** Cel mai important de reținut este faptul că, în cazul concursurilor organizate pe Facebook sau Instagram, nu este permisă condiționarea intrării în concurs de „tag-uirea” unei alte persoane sau ca respectivul concurs să se bazeze pe metoda tipică „share”.

Datele prelucrate prin intermediul activităților specifice parteneriatului Operator-Împuternicit privitoare la concursuri vizează operațiuni cu datele de tipul „single purpose” astfel încât după fiecare activitate aferentă obiectului contractului datele colectate și stocate în vederea desemnării câștigătorului sunt eliminate după încetarea operațiunii, dar nu mai tarziu de 7 zile de la data încetării.

Promovarea produselor pe rețelele de socializare

Societățile prelucreză datele cu caracter personal din momentul exprimării consimțământului din partea persoanelor fizice prin transmiterea datelor cu caracter personal prin intermediul secțiunii de comentarii, prin apăsarea butonului „LIKE” pentru pagină sau prin intermediul aplicației specifice de transmitere a mesajelor direct către societate (messenger).

Datele cu caracter personal trebuie să fie prelucrate de către societăți exclusiv în sensul consultării, nefiind stocate în evidențe separate și nefiind utilizate în alte scopuri decât cele pe care le au în vedere persoanele vizate atunci când accesează pagina de Facebook/Instagram.

În orice moment, persoanele vizate trebuie să poată opta la retragerea acordului pentru prelucrare prin intermediul retragerii opțiunii LIKE sau prin ștergerea comentariilor plasate voluntar la postările de pe paginile societății.

Datele nu vor fi dezvăluite către terți, cu excepția salariaților autorizați/mandatarilor care au ca atribuții în fișa postului prelucrarea de date cu caracter personal, în vederea promovării produselor societății.

În cazul în care pe site-ul unei societăți apar butoanele de legătură cu rețelele sociale (Linkedin, Facebook, Instagram, Twitter etc.) – de tip plug-in au de obicei ca rezultat înregistrarea imediată a adresei IP a vizitatorului, precum și înregistrarea comportamentului browser-ului folosit. Acest lucru poate apărea și dacă persoana vizată nu apasă butonul. Pentru a preveni acest lucru se poate folosi metoda „Shariff”. În acest caz, butoanele de social media vor stabili un contact direct între rețeaua socială și persoana fizică numai dacă respectiva persoană apasă (face click) pe respectivul buton de distribuire. Dacă persoana este deja conectată la o rețea socială, acest lucru se realizează fără o fereastră suplimentară pentru Facebook. Twitter afișează de obicei o fereastră pop-up în care textul mesajului tweet poate fi editat în continuare. În acest fel, persoana fizică poate publica conținutul în rețelele sociale fără ca aceste rețele să poată compila profiluri complete de navigare.

Un lucru ce trebuie amintit este acela că societățile pe a căror pagină sunt butoanele de Facebook, LinkedIn sau Twitter pot instala anumite coduri pentru a proteja datele utilizatorilor spre a nu fi transmise automat către societățile care dețin aceste rețele sociale (cum ar fi codul Shariff).

Abonarea la newsletter

Foarte multe societăți apelează la trimiterea unui newsletter către clienții lor și către persoanele interesate de produsele comercializate sau

serviciile prestate în scopul fidelizării acestora și de asemenea, pentru a-i anunța noutățile pe care le aduc.

Deși rata de deschidere a unui newsletter este relativ mică, foarte multe societăți apelează încă la aceasta formă de publicitate, pentru că presupune costuri relativ scăzute.

Fiind foarte simplu de urmărit dacă o persoană și-a dat consimțământul pentru a primi newslettere sau dacă o persoană nu a trimis o notificare privind retragerea consimțământului, sunt foarte multe provocări pentru societăți în ceea ce privește administrarea acestuia.

Astfel, prelucrarea datelor cu caracter personal se va face în general în baza consimțământului persoanelor vizate, în momentul abonării la newsletter și va viza activitatea de Marketing Direct a societății prin care se vor promova ofertele, campaniile și concursurile organizate de către societate. Bineînțeles, analizând de la caz la caz se vor putea trimite newslettere și în interes legitim.

Unele societăți aleg să înființeze un „club” al celor care sunt fani ai respectivului produs sau serviciu, în general acordând și diverse bonusuri sau avantaje celor din club. Bineînțeles, cei din club primesc și newslettere care îi informează periodic privind noutățile sau ce avantaje mai acordă compania respectivă. Pentru a intra în acest club trebuie să se respecte procedura descrisă mai sus de obținere a consimțământului.

Datele trebuie să nu fie dezvăluite către terți, cu excepția salariaților autorizați care au ca atribuții în fișa postului prelucrarea de date cu caracter personal, în vederea promovării produselor/campaniilor/concursurilor societății.



De reținut! Mesajele promoționale transmise de societate către personale vizate prin intermediul e-mailului vor trebui să fie însoțite, de fiecare dată, de un text care oferă posibilitatea persoanei vizate de a își retrage consimțământul de a îi fi prelucrate datele cu caracter personal și de a se dezabona de la serviciile newsletter.

Publicarea articolelor de presă

Se poate întâmpla ca articolele de presă să fie relevante și din punct de vedere GDPR. Astfel, se pot publica anunțuri de recrutare (am descris în capitolul privind Bunele practici în Departamentul de Resurse Umane ce trebuie să conțină acestea) sau diferite anunțuri privind promovările sau parteneriatele societății, în foarte multe cazuri aceste anunțuri fiind însoțite de fotografii ale persoanelor implicate.

Societățile ar trebui să se asigure că, anterior publicării articolelor în spațiul virtual, s-au comunicat, într-un mod transparent, persoanelor vizate scopul și temeiul prelucrării datelor cu caracter personal, inclusiv a imaginii persoanei vizate, drepturile acestora din urmă. Comunicarea trebuie să se realizeze printr-un mijloc ce asigură confirmarea primirii.

De foarte multe ori societățile aleg să colaboreze cu societăți de PR care le vor sprijini eforturile de a deveni cât mai vizibile. În acest caz, societatea de PR acționează ca un Împuternicit, iar în contractul cu această societate se vor specifica și obligații privind datele cu caracter personal ale persoanelor care vor apărea în comunicatele de presă.

Bune practici privind aplicarea GDPR-ului în domeniul Marketing

a. Persoana vizată are dreptul de a-și retrage consimțământul în orice moment, de aceea trebuie să i se ofere opțiunea de a-și schimba decizia și de a-și retrage cu ușurință consimțământul.

În ceea ce privește activitatea de newsletter, în fiecare comunicare comercială va fi pus la dispoziția persoanelor vizate un link pentru dezabonare.

De asemenea, în ceea ce privește cookie-urile de marketing și profilare, persoana vizată –vizitator site are opțiunea de a dezactiva aceste cookie-uri din setările browser-ului, fiind informat în mod corespunzător cu privire la această opțiune pentru toate tipurile de browser (Internet Explorer, Mozilla Firefox, Google Chrome, Safari).

b. Societatea nu trebuie să condiționeze participarea copilului la jocuri, primirea de premii sau orice alt tip de activitate promoțională de dezvăluirea de către acesta a mai multor date personale decât cele strict necesare pentru participare.

c. În cazul organizării de tombale publicitare este recomandată colectarea a cât mai puține date ale participanților – exemplu: nu este necesară colectarea datelor din Cartea de identitate (și mai ales a CNP-ului) a tuturor participanților, ci doar a câștigătorilor. E important să privim lucrurile prin prisma ideii că, atunci când se realizează o prelucrare de date, acestea trebuie reduse la minimul necesar.

d. Practicile anterioare Regulamentului NU sunt considerate din mai 2018 ca un acord al utilizatorului sub noua legislație. Altfel spus, lipsa unei acțiuni (spre exemplu: anunțuri de tipul „Navigarea pe acest site reprezintă acordul dvs. cu privire la politica de utilizare a cookie-urilor”) sau căsuțele pre-bifate trebuie înlocuite cu semnalări conform noii legislații.

e. Accesul la datele cu caracter personal arhivate ar trebui să se facă doar pe baza parolilor și este permis doar persoanelor din cadrul departamentului de marketing (salariați/mandatari) și atunci când este cazul, unor persoane autorizate din cadrul agențiilor de publicitate/societăților cu activități specifice de marketing (de exemplu, în cazul concursurilor).

În vederea asigurării securității datelor personale transmise către agențiile de publicitate, vă recomandăm crearea de e-mailuri separate, securizate cu parole la care au acces doar persoanele autorizate din cadrul agențiilor de publicitate/societăților cu activități specifice de marketing.

f. Trebuie instituită o procedură clară pentru cazul în care un angajat din cadrul departamentului de marketing constată că datele cu caracter personal au fost supuse unor acțiuni ilicite de accesare astfel încât orice angajat din Departamentul de marketing să știe cui trebuie să raporteze. De asemenea, dacă angajații/mandatarii din cadrul departamentului de marketing vor constata că a avut loc o breșă de securitate, trebuie să aibă un termen limită specificat pentru raportare.

Este foarte important de specificat în respectiva Procedură inclusiv cum are loc accesul în birourile/spațiile unde se desfășoară activitatea de marketing, unde se regăsesc și sistemele informaționale prin care se prelucrează datele cu caracter personal sunt restricționate, fiind permis accesul doar persoanelor care au autorizația necesară și nivelul de acces pentru prelucrare.

g. După retragerea consimțământului din partea persoanei vizate, aceasta din urmă este bine să primească un text (ideal ar fi să se trimită automat, printr-o procedură presetată), astfel încât persoana să fie încunoștințată de faptul că toate datele sale colectate și prelucrate în scop de Marketing i-au fost șterse.

h. Orice formular prin care utilizatorul își introduce datele personale cum ar fi abonarea la newsletter, crearea unui cont, plata electronică pe site, formularul de contact trebuie să fie însoțite de o notificare de confidențialitate cu trimitere la Politica privind confidențialitatea (și către pagina privind Datele cu caracter personal dacă aceasta există separat).

i. Recomandăm implementarea pe site a formularelor de solicitare a exercitării drepturilor persoanei vizate pentru a fi cât mai ușor să se depună o cerere (fără a limita exercitarea drepturilor la această formulă).

Departamentul de Vânzări

În cadrul fiecărei societăți există departamente aflate în prima linie a relațiilor cu clienții, partenerii sau angajații, pentru care GDPR vine cu o

serie de provocări specifice domeniului de activitate, a căror rezolvare este definitorie pentru buna funcționare a societății.

Departamentul de vânzări lucrează în general cu obiective clar precizate (target-uri), de multe ori câștigul fiecărui angajat depinzând de îndeplinirea obiectivului respectiv, astfel încât tentația angajaților în Departamentul de vânzări este de a folosi orice pistă (lead), indiferent că datele respectivei persoane au fost obținute în mod legal sau nu.

Astfel, vânzătorii lucrează cu liste de prospekți, își împărtășesc de multe ori aceste liste unul altuia din societăți diferite (acest lucru întâmplându-se mai ales în cazul foștilor colegi care păstrează legătura și își trimit unul altuia baze de date de la societatea la care lucrează).

Vom analiza pe rând aceste comportamente, insistând, ca de fiecare dată, pe importanța redactării unei Politici scrise special pentru Departamentul de vânzări și, de asemenea, instruirea periodică a angajaților din Departamentul de Vânzări în ceea ce privește datele pe care le pot folosi, cum se colectează în mod legal aceste date, dacă și în ce condiții se poate împărtăși baza de date etc.

Datele cu caracter personal prelucrate care se prelucrează de către Departamentul de Vânzări

Departamentul de vânzări din companie colectează și prelucrează în general următoarele date cu caracter personal:

- Numele și prenumele persoanei de contact (fie dintr-o companie dacă se vând produse Business to Business, fie ale clienților finali – dacă produsele/serviciile societății se adresează persoanelor fizice);
- Adresa de e-mail a persoanei vizate;
- Numărul de telefon;
- Adresa de domiciliu (dacă vorbim de cazurile tot mai rar întâlnite ale vânzătorilor din ușă în ușă);
- Adresa indicată de persoana vizată (în acest caz discutăm de adresa comunicată expres de client pentru livrarea unui produs comandat);
- Ce produse/servicii a achiziționat persoana respectivă (este important pentru o eventuală vânzare subsecventă sau pentru profilare);
- Data de naștere (consultanții de asigurări, în fapt tot vânzători, consideră foarte utilă această dată de naștere, atât pentru a ține legătura cu clientul, cât și pentru a-l profila).

În general Departamentul de vânzări păstrează doar o parte din aceste date, deși am întâlnit Departamente de vânzări foarte bine

organizate cu mii de contacte, fiecare dintre aceste persoane de contact având o foarte mare detaliere (ce a cumpărat, ce preferințe are, cum i s-a părut persoana vânzătorului respectiv, data nașterii, rude și datele de naștere ale rudelor etc.).

În cazul în care aceste date sunt obținute în mod legal (fie ca urmare a desfășurării unui contract, fie după obținerea unui consimțământ), nu este nicio problemă – problema se pune atunci când baza de date există, dar nu se mai știe în urma căror acțiuni a fost adăugată fiecare informație. În acest caz, este recomandabil să se analizeze fiecare contact și dacă nu subzistă un temei legal, să se procedeze la a se șterge contactele respective.

Este recomandabil ca la momentul respectiv să se întocmească un proces verbal în care să se menționeze câte contacte au fost șterse și pe ce bază (temei legal) au rămas contactele păstrate. Apoi, în Politica privind datele cu caracter personal în Departamentul de Vânzări să se precizeze care sunt pașii pentru a adăuga persoane sau informații noi despre o persoană în baza de date.

Temeiurile prelucrării datelor cu caracter personal

În cazul în care prelucrarea datelor cu caracter personal se bazează pe consimțământul persoanei vizate, toate detaliile precizate în cadrul subcapitolului privind obținerea consimțământului și păstrarea consimțământului rămân valabile.

În cadrul departamentului de vânzări poate să apară în schimb un alt temei pentru prelucrarea datelor – respectiv acela al executării unui contract.

Articolul 6 alin. (1) lit. (b) din GDPR indică un temei pentru prelucrare în cazul în care:

„Prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a lua măsuri premergătoare contractului, la cererea persoanei vizate”.

În acest sens, Departamentul de Vânzări poate colecta și prelucra datele unor persoane astfel încât să ofere sprijin pentru viitor (în anunțarea apariției unui model nou, prezentarea unor consumabile etc.) sau când nu s-a încheiat încă un contract cu persoana vizată, dar se negociază oferta sau trebuie luată o măsură precontractuală pentru a se încheia contractul (exemplu: măsurători, analize etc.) și trebuie ca datele să fie prelucrate pentru a face acest lucru.

Deci, este în regulă să se păstreze de către Departamentul de Vânzări informații referitoare la: numele persoanei care a încheiat contractul sau a cerut oferta, obiectul contractului sau al ofertei, ce s-a discutat în cadrul eventualei întâlniri (în temeiul executării contractului), dar nu și data nașterii sau adresa dacă nu există un consimțământ valabil obținut.

A fi „necesară” nu înseamnă că prelucrarea trebuie să fie esențială pentru realizarea unei activități contractuale sau pentru luarea unor măsuri precontractuale, însă acest temei nu se aplică dacă există alternative rezonabile și mai puțin intruzive.

O mare provocare a persoanelor care lucrează în Departamentul de Vânzări o reprezintă găsirea de potențiali clienți (lead-uri) fără a încălca normele GDPR. S-a discutat intens dacă sunarea la un număr afișat pe site-ul unei societăți respectă principiile GDPR sau nu. Noi considerăm că datele unei societăți (inclusiv număr de telefon sau adresele de e-mail de tip office@ sau secretariat@) nu intră în sfera de protecție GDPR, putând interfera cel mult cu legea nr. 365/2002 privind comerțul electronic, republicată în 2006.

Bune practici ale Departamentului de Vânzări în domeniul datelor cu caracter personal

a. În cazul în care se consideră că prelucrarea este necesară pentru încheierea/desfășurarea contractului, trebuie să informați persoanele vizate despre acest lucru (incluzând informații despre scop și temei în notificarea dvs. de confidențialitate/politica de confidențialitate/ contract).

b. Este important, de asemenea, a avea grijă la principiul minimizării datelor – chiar dacă persoana vizată și-a dat acordul, acest lucru nu înseamnă păstrarea unor date inutile.

De exemplu, este în regulă să se colecteze și prelucreze data de naștere dacă societatea are sau intenționează să desfășoare un program de loializare clienți prin trimiterea unei felicitări sau a unui cadou de ziua de naștere și dacă bineînțeles persoana își dă consimțământul, dar nu doar pe principiul „le stocăm că cine știe când ne trebuie”.

c. Având în vedere faptul că pentru oamenii de vânzări bazele de date reprezintă „aur”, subliniem încă o dată importanța informării și instruirii acestora asupra normelor GDPR, explicându-le de asemenea și riscurile cărora li se supune societatea, în cazul în care nu respectă politica de confidențialitate a societății.

Noi recomandăm ca, în cadrul instruirii, să li se prezinte o listă cu ce au voie și ce nu au voie să facă.



Exemplu:

AȘA DA

- Puteți contacta clienți ai societății pentru a le prezenta oferta de consumabile;
- Puteți suna persoanele prezente la expoziția de prezentare care și-au dat acordul pe formularul de consimțământ;
- Puteți suna la numărul de telefon al societăților afișat pe site-ul de prezentare al acestora pentru a cere acordul pentru trimiterea unei prezentări;
- Datele trebuie folosite doar în scopul pentru care persoana și-a dat consimțământul.

AȘA NU

- Nu copiați baze de date de la alte societăți;
 - Nu trimiteți baza de date a Departamentului/Societății altor persoane fără acordul Responsabilului de Date cu caracter personal;
 - Nu cumpărați baze de date care conțin date cu caracter personal;
 - Nu sunați persoane fizice („cold call”) dacă nu ați obținut acordul acestora.
- d. Regula demonstrării primirii consimțământului se păstrează, societatea fiind obligată să poată demonstra faptul că a primit consimțământul în mod legal pentru a le procesa informațiile.

Departamentul de Client Support

Departamentul de customer service, customer care, customer support sau relații cu clienții poate avea diferite denumiri, însă toate îndeplinesc aceeași funcție: descriu un departament crucial într-un business, responsabil pentru reputația brandului pentru care lucrează.

În multe societăți nu există un departament special de Client Support, atribuțiile acestuia fiind preluate de departamentul de Vânzări. În acest caz, toate obligațiile menționate mai sus subzistă, neexistând o bază de date separată.

Pentru situația în care acest departament este separat în cadrul societății, de obicei există și o bază de date ce conține datele clienților existenți pentru a-i ajuta în privința diferitelor solicitări (de la partea tehnică – atunci când nu funcționează ceva, până la facturare sau garanții).

Important este că există o bază de date specială, cu care lucrează angajații din acest departament.

Datele cu caracter personal prelucrate care se prelucrează de către Departamentul de Client Support

Departamentul de Client Support din companie colectează și prelucrează, în general, următoarele date cu caracter personal:

- Numele și prenumele persoanei de contact (fie dintr-o companie dacă se vând produse Business to Business, fie ale clienților finali – dacă produsele/serviciile societății se adresează persoanelor fizice);
- Adresa de e-mail a persoanei vizate;
- Numărul de telefon;
- Adresa indicată de persoana vizată (în acest caz discutăm de adresa comunicată expres de client pentru livrarea unui produs comandat);
- Ce produse/servicii a achiziționat persoana respectivă și când (sunt importante aceste date pentru servizare, garanții etc.). Singura întrebare care poate apărea aici este dacă se realizează o profilare a clienților în funcție de ce au cumpărat și dacă este legitimă această profilare – persoanei care a achiziționat o mașină de lux full option o să i se sugereze cauciucuri de iarnă de preț mic, mediu sau cele mai scumpe?

Temeiul prelucrării datelor cu caracter personal

Aici este evident un singur temei, și anume acela al executării contractului, întrucât persoanele care lucrează în acest departament discută doar cu actuali clienți ai societății. Fie că vorbim de clienți ai unui serviciu aflat în derulare (servicii de telefonie de exemplu) sau ai unui produs de folosință îndelungată (cum ar fi a unei piscine), persoanele de la Client Support își cunosc interlocutorii și aceștia se bucură de existența bazei de date, nemaitrebuind să povestească tot despre produsul/serviciul achiziționat.

Bune practici ale Departamentului de Client Support în domeniul datelor cu caracter personal

a. Cea mai întâlnită întrebare este cea legată de durata păstrării datelor cu caracter personal. Foarte multe societăți înțeleg să nu șteargă

niciodată aceste date – dorind să se folosească de informații în cazul în care clientul se întoarce. Nu este o alegere înțeleaptă, știut fiind faptul că normele GDPR impun limitarea în timp a prelucrării datelor cu caracter personal.

Noi recomandăm păstrarea datelor de către Departamentul de Client Support cât timp nu încetează contractul pentru servicii și pe perioada garanției pentru produse.

b. De foarte multe ori se externalizează acest serviciu și către ambasadori ai brandului – influenceri relevanți din domeniu, care pot cunoaște suficient de bine răspunsul la întrebări venite din partea utilizatorilor care preferă să vorbească direct cu aceștia; de exemplu, liniile aeriene apelează la bloggerii de călătorii ca aceștia să răspundă în legătură cu promoțiile ce urmează sau tips & tricks pentru a achiziționa bilete de avion, dar și către societăți care se ocupă cu aceste servicii, astfel încât acționează ca un împuternicit al societății (clienților fiindu-le comunicate datele prestatorului respectiv). În acest caz este foarte important contractul încheiat cu împuternicitul și bineînțeles verificarea acestuia înainte.

c. Atunci când serviciul se desfășoară în cadrul companiei, este foarte important softul folosit – trebuie verificat, de asemenea, dacă producătorii acestuia s-au conformat normelor GDPR.

d. Nu în ultimul rând este relevantă Procedura privind Datele cu Caracter personal ce trebuie implementată la nivelul Departamentului de Client Support și instruirea periodică a angajaților din acest departament.

Informarea persoanelor vizate asupra drepturilor pe care acestea le au

Drepturile persoanei vizate reprezintă nucleul Regulamentului privind Datele cu Caracter Personal, inclusiv al Departamentului de Marketing, iar implementarea metodelor de asigurare a posibilității de exercitare a acestor drepturi trebuie să fie un interes major al societăților – în orice caz, cele mai multe sesizări și plângeri vin din cauza nerespectării de către companii a acestor drepturi.

Regulamentul recunoaște persoanelor vizate o serie de 8 drepturi importante (societățile sunt cele obligate să se asigure de respectarea lor):

1. Dreptul la informare – art. 13 și 14 GDPR. Persoanele vizate trebuie să știe cum le sunt utilizate datele, chiar de la momentul la care se face colectarea. De principiu, acest drept este respectat prin comunicarea unei Note de informare (atunci când prelucrarea nu se întemeiază pe

consimțământ) sau prin semnarea unui Acord de prelucrare a datelor cu caracter personal (atunci când prelucrarea se întemeiază pe consimțământ). De asemenea, Persoana vizată trebuie să știe dacă datele îi sunt transferate sau dezvăluite, către cine și ce drepturi și obligații au persoanele în cauză cu privire la datele prelucrate.

Este un drept fundamental stipulat de GDPR și cele mai multe amenzi au fost date întrucât societățile nu au respectat acest drept al persoanelor ale căror date au fost colectate.

2. Dreptul de a avea acces la datele personale – art. 15 GDPR. Persoanele vizate pot solicita din partea societății confirmarea că se prelucrează sau nu date cu caracter personal care le privesc și, în caz afirmativ, pot primi acces la datele respective și la informațiile utile referitoare la acestea, într-un format utilizat în mod curent și care poate fi citit automat.

Modul de răspuns la exercitarea dreptului de acces se detaliază în general în Procedura de acces la date (parte integrantă din Termeni și Condiții sau din Politica de Confidențialitate dacă aceasta se regăsește separat de Termeni și Condiții, fiind prezentă pe site-ul societății, dar și în Politicile societății privind datele cu caracter personal).

3. Dreptul la ștergerea datelor – art. 17 GDPR. Persoanele vizate pot obține ștergerea datelor cu caracter personal. O astfel de cerere poate fi refuzată doar în anumite situații, cum ar fi atunci când datele sunt prelucrate pentru îndeplinirea unei obligații legale sau a unui interes legitim, care prevalează. Compania trebuie să comunice baza legală a unui refuz în termen de 30 de zile de la data comunicării solicitării în mod complet și legitim.

În general, departamentul de Marketing nu se poate prevala de îndeplinirea unei obligații legale – poate cu excepția păstrării datelor unui câștigător, în cazul în care premiul depășește 600 lei pentru care trebuie păstrate datele în scop financiar-contabil (de raportare a impozitului).

Altfel, dacă o persoană a cărei date sunt colectate și prelucrate solicită ștergerea acestora, societatea nu va putea refuza și trebuie să se asigure că datele au fost cu adevărat șterse.

4. Dreptul la rectificarea datelor – art. 16 GDPR. Atunci când apreciază necesar, persoanele vizate pot obține rectificarea sau completarea datelor cu caracter personal inexacte care le privesc.

5. Dreptul la restricționarea datelor – art. 18 GDPR. În unele situații, persoanele vizate se pot opune temporar la prelucrare (inclusiv la ștergere), atunci când o astfel de suspendare este necesară pentru

constatarea, exercitarea sau apărarea unui drept în fața anumitor autorități sau în instanța de judecată.

6. Dreptul la portabilitatea datelor – art. 20 GDPR. Orice persoană vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului (care le prelucrează în temeiul unui contract ori în temeiul consimțământului, prin mijloace automate) într-un format structurat, utilizat în mod curent și care poate fi citit automat, precum și dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal.

7. Dreptul la opoziție la prelucrarea datelor care ar putea produce prejudicii art. 21 GDPR. Orice persoană vizată are dreptul de a se opune prelucrării datelor sale personale, atunci când acestea îi pot produce prejudicii sau atunci când sunt prelucrate în scop de marketing direct.

Din acest motiv, toate newsletterele comunicate de Companie se vor trimite numai în baza consimțământului explicit, manifestat la momentul introducerii datelor de contact pentru transmiterea newsletter-ului, cu posibilitatea de dezabonare.

8. Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

Pe lângă aceste drepturi prevăzute unitar de GDPR, mai există un drept care poate fi exercitat de persoanele vizate și care trebuie menționat, respectiv acela de a depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal. B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, cod poștal 010336, București, România (pe adresa de email A.N.S.P.D.C.P.@dataprotection.ro).

Dintre toate, cele mai mari implicații în Departamentele de Marketing, cel de Vânzări și cel de Client Support îl are dreptul la informare. Informarea persoanelor fizice se face în general prin Politica de confidențialitate afișată pe site-ul societății și, de asemenea, reprezentanții tuturor celor 3 departamente enumerate mai sus trebuie să aibă mereu în vedere dreptul la informare atunci când colectează datele personale.

Persoanele vizate trebuie să știe, chiar de la momentul la care se face colectarea, modul în care se vor utiliza acele date, către cine vor fi ele dezvăluite ori transferate, ce drepturi au persoanele în cauză cu privire la datele prelucrate etc.

Este important de reținut că informarea trebuie realizată, indiferent de temeiul utilizat pentru realizarea prelucrării (interes legitim sau consimțământ pentru departamentele de Marketing și Vânzări, interes contractual,

interes legitim sau consimțământ în ceea ce privește Departamentul de Client Support).

Vom reveni asupra lor în capitolul ce tratează măsurile tehnice și organizatorice, important de reținut pentru moment este că, fiind un drept esențial al persoanelor fizice, în contextul datelor cu caracter personal, trebuie acordată o grijă deosebită acestei informări în orice context de colectare și prelucrare date pentru Marketing, Vânzări sau Client Support.

Un alt lucru care trebuie reținut este că aceste departamente trebuie să actualizeze periodic informarea privind drepturile persoanelor vizate.

Operatorul este obligat să răspundă cererilor de exercitare a drepturilor, indiferent dacă decide să se conformeze acestora sau nu. Astfel, conform GDPR, operatorul trebuie să răspundă fără întârzieri nejustificate și cel târziu în termen de o lună de la primirea cererii, însă conformarea cu cererea depusă depinde de temeiul juridic în baza căruia s-a făcut prelucrarea. Astfel, dacă operatorul respectă o obligație legală, se află în executarea unui contract, sau acționează în baza unui interes legitim temeinic justificat este posibil să nu aibă posibilitatea de conformare cu cererea depusă. De exemplu, dacă premiul în cadrul unui concurs publicitar este mai mare de 600 de lei, datele câștigătorului vor fi păstrate în scop fiscal-contabil chiar dacă acesta va solicita ștergerea datelor sale.

Informarea privind drepturile persoanelor vizate se poate face online, pe site-ul companiei/concursului/brandului respectiv, dar și offline, prin intermediul Acordului de prelucrare a datelor cu caracter personal care trebuie să se regăsească în locul unde se colectează datele cu caracter personal (în cadrul expoziției, cursului sau evenimentului în care persoanele își lasă datele pentru o informare ulterioară) pentru a fi studiate la cerere. Având în vedere riscurile inerente păstrării acestora într-un loc în care au acces mai multe persoane, este bine ca societatea să menționeze în procedurile sale privind confidențialitatea datelor măsuri de siguranță în privința acestora.

MĂSURI TEHNICE ȘI ORGANIZATORICE

„Oamenii acceptă schimbarea numai atunci când se confruntă cu necesitatea și recunosc necesitatea doar atunci când o criză se abate asupra lor”.

Jean Monnet

Un principiu cheie GDPR presupune ca operatorul să prelucrez datele cu caracter personal prin intermediul unor măsuri „tehnice și organizatorice adecvate”¹¹ sau, după caz, „adevate și eficiente, în măsură să demonstreze conformitatea activităților de prelucrare, inclusiv eficacitatea măsurilor”¹².

Identificarea sau, după caz, crearea și implementarea unor măsuri tehnice și organizatorice reprezintă o adevărată provocare pentru companii, mai ales dacă privim la practica recentă a autorității, unde lipsa unor măsuri tehnice și organizatorice corespunzătoare a fost sancționată.

În termeni generali, măsurile tehnice și organizatorice reprezintă acțiunile organizației cu privire la procesele de prelucrare. În continuare, vom oferi o serie de orientări în direcția implementării unor măsuri tehnice și organizatorice menite să asigure securitatea datelor cu caracter personal prelucrate la nivel de companie.

Bunele practici în materie de măsuri tehnice și organizatorice adoptate la nivelul companiei se pot dovedi însă insuficiente sau necorespunzătoare în eventualitatea unei investigații, astfel încât se recomandă ca fiecare organizație să adopte măsuri specifice activității pe care o desfășoară pentru a garanta un grad ridicat de securitate în ceea ce privește datele cu caracter personal prelucrate.

Responsabilitatea operatorului. Privacy by design & by default

În linii mari, principiul responsabilității pe care îl regăsim în GDPR și care putea fi identificat și în legislația anterioară se referă la faptul că trebuie să dispuneți de mecanismele interne necesare pentru a demonstra conformitatea.

¹¹ Articolul 32 din Regulament.

¹² Considerentul (74) din Regulament.

Responsabilitatea nu trebuie privită ca fiind limitată strict la relația cu autoritatea, în eventualitatea unui control, ci și în relația cu terții. Există companii care, într-o primă etapă a negocierilor în vederea încheierii unui contract, solicită de la potențialul partener informații privind conformitatea cu cerințele GDPR, prin completarea unui *checklist* preliminar menit să identifice dacă cealaltă parte îndeplinește integral sau parțial o serie de măsuri tehnice și organizatorice minime în vederea asigurării confidențialității și securității datelor cu caracter personal ori după caz, dacă cealaltă parte își ia angajamentul ca până la finalizarea negocierilor și încheierea contractului să implementeze cerințele. În contextul în care minimizarea riscurilor și consolidarea unei bune reputații a companiilor au devenit esențiale, conformitatea cu cerințele GDPR a ajuns să reprezinte un adevărat avantaj competitiv în cadrul negocierilor contractuale.

Ce înseamnă „*by design*” în domeniul GDPR?

„*Data protection by design*” presupune existența unor măsuri tehnice și organizatorice care să asigure protecția datelor încă de la început, de la momentul conceperii mijloacelor de prelucrare.

O componentă importantă este anticiparea riscurilor și a evenimentelor care pot încălca confidențialitatea celor a căror date sunt prelucrate (clienți, angajați, parteneri etc.) înainte de apariția acestora și luarea de măsuri pentru a le preveni. Ar ajuta astfel ca în echipa de „proiectare” a noului produs sau serviciu să fie cooptat și un pesimist sau mai bine spus o persoană care își imaginează doar droburi de sare care cad peste copil, care să poată să se gândească cum ar putea fi încălcată confidențialitatea și apoi să se găsească măsuri pentru a combate această posibilitate.

Se insistă foarte mult pe utilizarea pseudonimizării (înlocuirea materialului identificabil personal cu identificatori artificiali) și a criptării (codificarea mesajelor astfel încât numai persoanele autorizate să le poată citi).



Exemplu: în momentul creării unui soft prin care un robot răspunde la telefon, dezvoltatorul softului trebuie să integreze confidențialitatea discuției, criptarea sau pseudonimizarea dacă este cazul, păstrarea datelor un timp limitat etc.

Ce înseamnă „*by default*” în domeniul GDPR?

„*Data protection by default*” presupune implementarea de garanții implicite de ordin tehnic și organizatoric pentru orice produs sau serviciu

cum ar fi limitarea accesului la date doar pentru persoanele care chiar au nevoie să lucreze cu ele.

Companiile ar trebui să se asigure în mod implicit că datele cu caracter personal sunt prelucrate cu cel mai ridicat nivel de protecție (adică numai datele necesare, perioadă scurtă de stocare, accesibilitate limitată), astfel încât datele cu caracter personal să nu poată fi accesate de un număr nelimitat de persoane („protecția datelor în mod implicit”).

Cu alte cuvinte, ar trebui să existe o preocupare continuă cu privire la protejarea datelor automat în orice sistem informatic, serviciu, produs și/sau sistem de afaceri, astfel încât să nu fie necesar ca persoanele fizice să întreprindă măsuri suplimentare pentru a-și proteja confidențialitatea.

Astfel, societățile ar trebui să proceseze numai datele cu caracter personal de care au nevoie pentru scopurile comunicate, și pe care le folosim doar pentru aceste scopuri (evitând folosirea pentru alte scopuri de care cei ale căror date sunt prelucrate nu știu).

!
 • **Exemplul 1:** O platformă pentru catering ar trebui încurajată să stabilească setările de profil ale utilizatorilor în modul cel mai favorabil confidențialității, limitând de la început accesibilitatea profilului utilizatorilor, astfel încât acesta să nu poată fi accesat în mod implicit de un număr nelimitat de persoane.

!
 • **Exemplul 2:** În cadrul unei grădinițe se stabilesc useri și parole pentru fiecare educator astfel încât accesul fiecăruia să fie limitat doar la datele copiilor din grupa sa.

Board-ul European pentru Protecția Datelor a lansat pe 13.11.2019, un ghid relevant în dezbatere publică cu privire la „*data protection by design*” și „*data protection by default*”.

Acest ghid stabilește care sunt măsurile pe care operatorii de date personale trebuie să le ia atunci când stabilesc mijloacele de prelucrare a datelor și ce garanții trebuie asigurate implicit:

• Operatorii trebuie să asigure transparența – de la început, trebuie să se asigure faptul că persoanele vizate de prelucrare (sau potențialele persoane vizate de prelucrare) trebuie să știe clar ce date le vor fi colectate, cum vor fi folosite aceste date și dacă vor fi comunicate altcuiva aceste date. Discutăm, aici, de o informare relevantă, la momentul oportun, care să fie făcută într-un limbaj simplu și clar, care să fie ușor accesibilă (pe mai multe canale, deci nu doar text scris) și care să fie completă.

Aceste lucruri ar trebui să se reflecte, de exemplu, în politica de confidențialitate, care să fie ușor de înțeles, să nu fie încărcată cu termeni tehnici și care, printre altele, să fie ușor accesibilă.

- **Legalitatea** – procesele de prelucrare și însăși conceperea lor trebuie să se facă prin luarea în considerare a temeiului legal pentru prelucrare – pentru societăți discutăm de consimțământ, interes legitim sau îndeplinirea obligațiilor contractuale, fără să fie exclusă posibilitatea reținerii datelor pentru îndeplinirea unei obligații legale, de exemplu.

Ce este important, însă, este identificarea temeiului obiectiv aplicabil și anticiparea relevanței lui, în timp, pentru a justifica prelucrarea continuă. Mai mult, trebuie identificat clar scopul prelucrării sau scopurile respectivei prelucrări.

- **Principiul prelucrării în mod echitabil** – practic, prelucrarea nu trebuie să aibă scop discriminatoriu și nici să inducă în eroare persoanele vizate. De asemenea, trebuie să se urmărească previzibilitatea prelucrării, în ceea ce privește persoanele vizate și evitarea consecințelor negative față de acestea. Acest lucru implică inclusiv o anticipare a efectelor prelucrării asupra stării generale a persoanei vizate. De exemplu, nu se poate încerca influențarea persoanelor în vederea acceptării prelucrării, în special dacă discutăm de activități online.

- **Limitarea clară a scopurilor** pentru care sunt prelucrate datele și alegerea mijloacelor necesare pentru atingerea lor – contează foarte mult stabilirea clară a scopurilor pentru care sunt prelucrate datele, identificarea mijloacelor necesare pentru atingerea lor și determinarea compatibilității prelucrărilor ulterioare cu scopurile stabilite inițial.

Concret, se mai poate discuta și de limitarea tehnică a refolosirii datelor, odată colectate, și de implementarea unor mecanisme de reanalizare continuă.



- **Exemplu:** Dacă anumite date sunt prelucrate de către un comerciant pentru îndeplinirea obligațiilor contractuale (cum ar fi adresa), aceste date nu vor putea fi prelucrate în alt scop ulterior. Ghidul dă exemplul unui soft care folosește datele colectate, pentru a stabili puterea de cumpărare a clienților și pentru a facilita procesul de marketing. Prelucrarea ulterioară nu este compatibilă cu scopul inițial.

- **Reducerea la minimum a datelor prelucrate** – acest principiu implică faptul că doar datele care sunt necesare, relevante și potrivite atingerii scopului pentru care se face prelucrarea vor fi colectate. Astfel, sistemele de prelucrare trebuie adecvate la scopul prelucrării.

! **Exemplu:** Când sunt achiziționate produse electronice (precum programe sau cărți în format electronic), nu va fi necesar numărul de telefon al cumpărătorului pentru vânzarea propriu-zisă a acelor produse. Astfel, inserarea casuțelor obligatorii cu privire la numărul de telefon al cumpărătorului, atunci când acesta completează un formular online pentru a finaliza comanda, nu este justificată. De asemenea, trebuie verificat constant dacă datele prelucrate își mențin necesitatea, în timp.

- Datele prelucrate trebuie să fie relevante și să reflecte realitatea – este importantă asigurarea măsurilor tehnice prin care să fie posibil menținerea unor date relevante și în acord cu realitatea.

- Limitarea stocării – practic, datele trebuie stocate atât timp cât este necesară identificarea persoanei în vederea atingerii unui anumit scop. Pentru aceasta, e nevoie o înțelegere adecvată a datelor prelucrate și a motivului pentru care sunt stocate acestea. Ideal ar fi implementarea unor soft-uri care șterg automat datele, la momentul în care acestea nu mai sunt necesare.

- Asigurarea integrității datelor și a confidențialității lor – asigurarea acestora permite prevenirea unor breșe de securitate, însă și asigură respectarea celorlalte principii. Acest lucru implică, mai ales, actualizarea constantă a cadrului de securitate.

GDPR impune companiilor în aplicarea acestui principiu¹³ implementarea unor măsuri tehnice și organizatorice corespunzătoare și a unor precauții necesare, menite să dea eficiență principiilor privind protecția datelor într-o manieră care să protejeze drepturile și libertățile persoanelor vizate.

Protecția implicită gândită din momentul proiectării unui sistem ce implică procese de prelucrări de date presupune integrarea noului sistem într-un circuit sigur ce își va menține securitatea pe toată durata de viață. Odată implementat un astfel de sistem, compania ar trebui să aibă în vedere cele mai riguroase setări de confidențialitate aplicabile în mod automat.

Privacy by design & by default presupune o abordare proactivă din partea operatorului care trebuie să privească protecția datelor ca parte integrantă din dezvoltarea tehnologică a companiei. În acest sens, vor fi identificate potențialele riscuri rezultate din implementarea unui nou sistem și vor fi create măsuri de remediere în cazul în care un risc identificat se

¹³ Articolul 25 din Regulament.

concretizează într-un incident de securitate. Mai departe, compania va reanaliza la anumite intervale de timp eficiența planului de remediere.

Eficiența stă la baza principiului *Privacy by design & by default*, aceasta fiind direct legată de obligația companiei de a demonstra conformitatea procesului de prelucrare.

Companiile nu sunt obligate să implementeze măsuri tehnice și adecvate noi, atât timp cât măsurile actuale sunt de natură a acoperi toate riscurile identificate în analiza noului sistem. Cu toate acestea, măsurile deja implementate ar trebui să fie concepute astfel încât să fie solide și să poată fi extinse în cazul creșterii riscurilor identificate sau care ar putea apărea pe parcursul utilizării sistemului.

Un prim aspect de avut în vedere în aplicarea principiului *Privacy by design & by default* este stadiul actual al tehnologiei. Așadar, operatorul va avea în vedere progresul în materie de mijloace tehnologice disponibile pe piață. Necunoașterea evoluției în acest domeniu ar putea duce la ineficiența măsurilor tehnice și organizatorice avute în vedere pentru implementarea sistemului.

De asemenea, va fi avut în vedere costul implementării, luând în calcul nu doar valoarea propriu-zisă a sistemului tehnic, ci și resursele puse la dispoziția implementării măsurilor adecvate precum resurse umane implicate sau timp alocat. Implementarea unor măsuri adecvate nu trebuie să conducă la ideea unor costuri ridicate însă în cazul în care principiile GDPR nu sunt respectate, imposibilitatea de a susține financiar mijloace adecvate de protecție nu va constitui o circumstanță atenuantă pentru operator la fel cum investițiile majore nu conduc neapărat și la ideea unei implementări efective a principiilor¹⁴.

Măsuri tehnice

Atunci când discutăm despre noțiunea de măsuri tehnice legate de protecția datelor cu caracter personal, ne gândim la componente hardware (serve, laptopuri, hard disk-uri), software (sisteme de operare, aplicații de business), canale de comunicare (WiFi, Internet) sau la documente fizice (printare, scanare, copiere). Într-adevăr, în ceea ce privește măsurile tehnice pe care compania are obligația să le implementeze pentru a asigura un nivel de protecție adecvat, ne vom raporta la aspecte de securitate a datelor, implementate, de regulă, de Departamentul IT.

¹⁴ Ghidul nr. 4 EDPB cu privire la art. 25 – Data Protection by Design and By Default.

Autoritatea de Supraveghere din Franța, CNIL (Comission Nationale de l'informatique et des libertes) propune, prin intermediul Ghidului „Security of Personal Data” elaborat în anul 2018, modele de măsuri tehnice ce prezintă un grad ridicat de securitate a datelor pe care companiile îl pot consulta anterior implementării de măsuri tehnice sau dacă vor să verifice eficiența sistemului deja implementat. Un prim aspect pe care CNIL îl supune atenției persoanelor care parcurg acest material constă în creșterea gradului de responsabilizare a persoanelor care intră în contact cu datele personale ale companiei. Așadar, societățile ar trebui să aibă în vedere o măsura organizatorică foarte importantă pe care urmează să o analizăm în secțiunea dedicată măsurilor organizatorice pentru ca măsurile tehnice să funcționeze în sensul intenției companiei de a duce la îndeplinire obiectivele stabilite în planul de acțiuni și anume instruirea personalului, resursa umană fiind elementul cheie în procesul de conformare a companiei.

De asemenea, în dezvoltarea precauțiilor de bază pe care companiile le pot avea în vedere, în completarea instruirii personalului, CNIL propune și elaborarea unui regulament și aplicarea lui obligatorie. Pentru a corela documentele de resurse umane deja existente la nivel intern cu aceste bune practici, companiile pot opta să revizuiască regulamentul intern, astfel încât să includă aspecte specifice protecției datelor cu caracter personal. Sigur, nu este nimic greșit în elaborarea unui regulament separat, cu reguli clare în materie de protecție a datelor însă din rațiuni practice, cele mai multe companii aleg să revizuiască regulamentul intern, prilej cu care pot trata și alte aspecte ce țin de relațiile de muncă.

! **Exemple de reguli de securitate pe care societatea le poate impune fie prin intermediul regulamentului intern, fie prin intermediul unui regulament distinct ori chiar prin intermediul unei politici interne IT:**

- angajații să nu divulge parolele individuale de acces pentru echipamente/aplicații, codul de acces în incintele societății etc.;
- în măsura în care angajații își pot stabili singuri parolele, să respecte o serie de criterii cu privire la complexitate (să aibă minim 8 caractere, să conțină un mix de caractere alfabetic, atât litere mari cât și litere mici și non-alfabetice etc.) și să schimbe parolele la intervale regulate de timp;
- angajații să nu instaleze aplicații fără autorizație din partea Departamentului IT/conducerii;
- angajații să nu lase mijloacele de lucru nesupravegheate și să aibă în vedere activarea funcției screen saver cu solicitare ulterioară de parolă de acces după un interval de timp foarte mic de inactivitate;

- angajații să închidă stațiile de lucru când părăsesc biroul, la finalul programului de lucru sau în cazul în care lipsesc mai mult de o ora etc.;
- să nu utilizeze mijloace de printare publice pentru documentele societății;
- să nu stocheze date personale pe stick-uri USB sau hard disk-uri externe;
- să nu dezactiveze programele anti-malware preinstalate pe stațiile de lucru;
- să nu utilizeze rețele de internet necunoscute;
- să utilizeze adresa de e-mail pusă la dispoziție de companie exclusiv în vederea îndeplinirii atribuțiilor.

Securizarea echipamentelor prin intermediul cărora se prelucrează date cu caracter personal

Autentificarea unică a membrilor personalului

Asocierea fiecărui angajat cu un identificator unic înainte de accesarea datelor cu caracter personal se poate materializa fie prin alocarea unei parole ori a unui cod de acces, fie prin alocarea unui profil recunoscut pe bază de date biometrice.

CNIL propune trei elemente de autentificare, după cum urmează:

- Ceva ce user-ul cunoaște, cum ar fi o parolă;
- Ceva ce persoana are, cum ar fi un card „smart”;
- Ceva ce persoana este sau face, cum ar fi amprenta digitală sau semnătura digitală.

Principiul „something you know” nu este limitat la propunerea CNIL, putând fi extins și către alte metode de autentificare, precum coduri PIN, întrebări de securitate, captcha și alte mecanisme similare. De asemenea, principiul „something you have” poate presupune, separat de cardurile „smart” și utilizarea de carduri de acces, token-uri de autentificare etc. Principiul „something you are” poate avea în vedere și alte metode de autentificare a unui utilizator în baza informației genetice a respectivului utilizator, cum ar fi amprenta vocală, recunoașterea facială, scanarea irisului etc.

De avut însă în vedere este faptul că utilizarea de mijloace biometrice pentru autentificare este supusă unei justificări întemeiate și demonstrării faptului că mijloacele de autentificare anterioare nu și-au dovedit eficiența.

În materie de parole și coduri de acces, CNIL recomandă o serie de măsuri pe care companiile le pot implementa, cele mai importante fiind următoarele:

- să conțină cel puțin 8 caractere, incluzând majuscule, minuscule, numere și caractere speciale, dacă metodele de autentificare includ restricții de tipul: blocarea temporară a contului după câteva introduceri greșite a parolei; introducerea unui cod Captcha; blocarea contului după 10 încercări eșuate;
- să conțină cel puțin 12 caractere și minimum 4 tipuri de caractere, dacă autentificarea se realizează doar pe bază de parolă;
- să conțină peste 5 caractere, dacă autentificarea presupune alte informații suplimentare confidențiale; pentru informațiile suplimentare se recomandă utilizarea unui identificator care să conțină cel puțin 7 caractere și blocarea contului după 5 încercări eșuate;

Pot fi avute în vedere doar 4 caractere dacă autentificarea vizează un echipament deținut de utilizator și dacă parola este folosită doar pentru deblocarea device-ului (de exemplu, un telefon mobil).

Ca bună practică, se recomandă schimbarea, de către salariat, a parolei pusă la dispoziție după prima logare pe contul individual.

În completarea aspectelor privind setarea parolelor, CNIL atrage atenția unor precauții suplimentare, în legătură cu care se recomandă ca societatea să depună toate diligențele:

- interzicerea comunicării parolelor asociate conturilor individuale alocate salariaților;
- interzicerea stocării parolei într-un document necriptat, pe o foaie sau într-o locație ușor accesibilă oricărei persoane;
- interzicerea salvării parolei în browser, fără utilizarea unei parole suplimentare (administrator);
- interzicerea utilizării unei parole ce conține date personale (nume, zi de naștere etc.);
- interzicerea utilizării aceleiași parole pentru mai multe conturi;
- interzicerea parolei implicite;
- interzicerea transmiterii parolelor prin intermediul e-mail-ului.

Exemplele de mai sus nu sunt limitative, fiind cele mai des întâlnite în practică la nivelul companiilor ce au implementat cerințele GDPR, inclusiv în materie de măsuri tehnice.

Separat de aspectele de mai sus, pot fi identificate, împreună cu Departamentul IT și alte măsuri tehnice care să asigure securitatea sistemelor.

Executarea copiilor de siguranță

Auzim frecvent noțiunea de backup în materie de măsuri de securitate. Având în vedere riscul ridicat ca informațiile să fie pierdute, societățile acordă o mare importanță backup-ului, adică executării de copii de rezervă a fișierelor. Fie că societatea optează pentru un sistem manual de backup, realizat de un specialist în domeniul IT la anumite intervale de timp, în funcție de solicitarea companiei (zilnic, săptămânal, bilunar, lunar), fie că se optează pentru un sistem automat de backup, realizat prin intermediul unui software dedicat, este important ca o astfel de măsură să fie implementată la nivel de companie pentru preîntâmpinarea incidentelor de securitate. În ultimul timp, majoritatea companiilor au optat pentru backup-ul în Cloud, situație în care datele sunt stocate în mediul online, prin oferirea de spațiu de găzduire.

În materie de backup, CNIL recomandă să se aibă în vedere elaborarea unui plan de continuitate a activității IT care să poată anticipa posibilele incidente (de exemplu, defectarea componentelor hardware) și care să facă referire inclusiv la persoanele implicate, efectuarea unei verificări a utilizatorilor, furnizorilor de servicii și a subcontractorilor în materie de gestionare a incidentelor de securitate și efectuarea de testări regulate pentru restabilirea copiilor de rezervă și aplicarea planului.

În materie de echipamente, se recomandă ca societatea să folosească o sursă de alimentare neîntreruptă pentru a proteja echipamentul utilizat.

Trebuie evitată păstrarea copiilor de siguranță în același loc cu echipamentele care găzduiesc datele personale, deoarece o pierdere de date care ar putea să apară în locația respectivă ar putea conduce la pierderea definitivă a datelor.

Anticiparea incidentelor de securitate ce ar putea rezulta din pierderea sau furtul unui echipament

În contextul în care mediul în care lucrăm devine din ce în ce mai digitalizat, automat cresc și riscurile asociate prelucrărilor de date. Compania trebuie să aibă în vedere evitarea, pe cât posibil, a acestor riscuri.

CNIL propune o serie de măsuri generale, de exemplu, aplicarea de măsuri de criptare pentru a proteja dispozitivele mobile de lucru și pe cele de stocare externă (laptop-uri, stick-uri USB, hard disk-uri externe etc.) prin

criptarea dispozitivului în întregime, dacă este posibil, criptarea individuală a fișierelor, crearea de arhive criptate etc., dar și o serie de măsuri suplimentare, de exemplu aplicarea unui filtru de protecție pe ecranele dispozitivelor folosite în spații publice sau limitarea capacității de stocare a datelor pe dispozitivele mobile la ce este strict necesar și dacă este posibil, interzicerea folosirii echipamentelor pe care sunt stocate date personale în călătoriile în străinătate.

În ceea ce privește telefoanele smart, suplimentar de codul PIN, se recomandă blocarea automată a dispozitivului și solicitarea suplimentară de informații pentru deblocare (o parolă sau un contur etc.).

Tehnologia actuală permite dezvoltarea unor sisteme menite să protejeze informațiile stocate pe mediile de lucru aparținând companiei, prin intermediul unor sisteme ce permit un control eficient în ceea ce privește securitatea informației.

! **Exemplu:** compania pune la dispoziția angajaților laptopuri/ tablete ce prezintă un sistem ce permite IT-ului să blocheze instant echipamentul în caz de pierdere ori furt. Utilizarea unor astfel de soluții tehnice conduce la diminuarea riscurilor rezultate din incidentul de securitate.

Securizarea serverelor

Având în vedere faptul că serverele stochează o cantitate mare de date cu caracter personal, se recomandă ca întărirea măsurilor de securitate aplicate acestui segment să fie o prioritate pentru companii.

CNIL propune o serie de precauții de bază în această direcție, precum permiterea accesului la instrumente și interfețe doar pentru persoanele autorizate, adoptarea unei politici specifice de alocare a parolelor pentru administratori, schimbare parolei de fiecare dată când un administrator părăsește compania sau există suspiciuni în sensul în care sistemul ar putea fi compromis, evitarea utilizării de servicii nesecurizate (autentificate cu text clar, flux de text etc.), evitarea utilizării serverelor care găzduiesc baze de date pentru alte funcții, în special pentru a naviga pe site-uri web, pentru a accesa mesageria electronică etc., evitarea amplasării bazelor de date direct pe un server accesibil de pe Internet ori partajarea parolei de administrator între mai mulți administratori.

Suplimentar de bunele practici în materie de securizare a serverelor prevăzute mai sus, CNIL propune ca operațiunile de administrare a

serverului să se efectueze prin intermediul unei rețele dedicate și izolate, accesibilă numai după o autentificare puternică și cu o trasabilitate sporită și ca accesul de la distanță să fie restricționat.

Protejarea rețelei interne de internet

În materie de protejare a rețelelor interne, există multiple îndrumări practice, urmând să exemplificăm, în cele ce urmează, cele mai importante bune practici pe care companiile ar trebui să le implementeze:

- limitarea accesului la rețea (CNIL propune blocarea funcțiilor neesențiale);
- filtrarea traficului intern prin utilizarea de firewall, proxy etc.;
- utilizarea unor metode corespunzătoare de criptare a rețelelor wireless (CNIL propune utilizarea criptării de ultimă generație – WPA2 sau WPA2-PSK cu parolă complexă);
- evitarea utilizării criptării de tip WEP pentru securizarea conexiunilor wireless;
- utilizarea tehnologiei VPN (Virtual Private Networks), în cazul accesării rețelei interne prin intermediul mijloacelor la distanță, precum și implementarea unei tehnici îmbunătățite de autentificare (**exemplu:** implementarea a doi factori de autentificare, ca măsură suplimentară de protecție a sistemului informatic al unei companii).

Suplimentar, CNIL propune, ca precauții suplimentare, implementarea unui mecanism de identificare automată a echipamentelor utilizând identificatori de card de rețea pentru a limita accesul dispozitivelor neautorizate și a unui sistem de detectare a intruziunilor astfel încât să poată fi identificate eventualele atacuri.

ISO27 001:2013

Cel mai cunoscut standard internațional privind sistemul de management al securității informației în momentul de față este ISO 27001:2013.

Acest standard are ca scop evaluarea eficienței sistemului de management al securității informației și implicit, de a oferi cerințe specifice menite să asigure implementarea unui sistem eficient de management al securității informației.

ISO 27 001 poate fi avut în vedere împreună cu alte standarde de management, cum ar fi ISO 9000 și 20 000, având mai multe puncte comune.

Standardul tratează aspecte precum organizarea securității informației, securitatea resurselor umane, managementul bunurilor/resurselor, managementul accesului, securitatea fizică, securitatea operațională, securitatea comunicațiilor, relația cu furnizorii, achiziția, dezvoltarea și mentenanța sistemelor, managementul incidentelor privind securitatea informației, conformitatea generală a organizației etc.

Este important de avut în vedere ca implementarea ISO 27 001 la nivelul unei companii instituie o prezumție de „nevinovăție” în favoarea companiei atunci când intervine o breșă de securitate. Tocmai de aceea, ca bună practică, se recomandă implementarea acestui standard la nivelul companiilor. Un alt standard eficient în materie de securitate este ISO 27 701 care completează cerințele de securitate prevăzute de ISO 27 001 și ajută la conformarea operatorului cu prevederile Regulamentului. Operatorul care a implementat standardul 27 001 poate extinde măsurile implementate astfel încât cerințele standardului 27 701 să fie îndeplinite.

Măsurile organizatorice

Planul de conformare

Planul de conformare pentru companie poate fi întocmit în urma efectuării unui audit privind conformitatea operatorului, pe baza rezultatelor din raportul de audit. Desigur, în ipoteza în care nu a fost realizat un audit, planul poate avea ca punct de plecare chiar această etapă preliminară.

Întocmirea unui plan de conformare nu este prevăzută ca obligație legală, acest instrument inclus în categoria bunelor practici putând constitui o dovadă suplimentară în demonstrarea conformității companiei.

Un astfel de document ar putea cuprinde strategia companiei pentru o durată determinată (de exemplu, un an) sau ar putea fi gândit pentru o perioadă mai lungă, urmând să fie actualizat periodic în funcție de anumite aspecte precum apariția unor acte normative cu impact asupra societății, introducerea unor mijloace tehnice noi în activitate, modificări organizaționale etc.

În funcție de anumite criterii precum activitatea societății, volumul de date prelucrate, stadiul conformității, planul ar putea fi structurat fie pe pași de urmat în asigurarea conformității companiei, în funcție de priorități sau pe diferite structuri interne:

! **Exemplul 1:** Planul de conformare 2020-2021 vizează următoarele etape:

1. Realizarea unui audit preliminar care să identifice nivelul actual al conformității societății;
2. Desemnarea unui DPO;
3. Realizarea DPIA pentru procesele de prelucrare în care intervine obligația legală cu privire la întocmirea acestui document;
4. Informarea persoanelor vizate privind existența unor mijloace video și a unor mijloace de localizare geografică;
5. Revizuirea documentelor privind protecția datelor pentru site și introducerea unui mecanism care să permită bifarea cookie-urilor;
6. Implementarea documentelor specifice pentru salariați;
7. Realizarea unui audit pentru identificarea eventualelor vulnerabilități și stabilirea planului de conformare pentru anul următor.



● **Exemplul 2:**

1. Implementarea documentelor specifice pentru Departamentul HR: semnarea notelor de informare a salariaților, semnarea actelor adiționale, revizuirea și comunicarea regulamentului intern revizuit;
2. Implementarea documentelor specifice pentru mijloacele de supraveghere video;
3. Instruirea salariaților din Departamentul HR;
4. Redactarea și semnarea DPA-urilor;
5. Instruirea salariaților din Departamentul Marketing;
6. Analiza mijloacelor noi de prelucrare în vederea identificării proceselor ce ar impune întocmirea DPIA;
7. Revizuirea anuală a Politicii de Confidențialitate și a Politicii de Cookie-uri;
8. Redactarea unei politici de acces în unitățile de producție;
9. Actualizare registru de prelucrare;
10. Realizare auditului periodic și întocmirea raportului de audit.



● **Exemplul 3:**

1. Realizarea unui audit care să identifice nivelul actual al conformității societății;
2. Actualizarea politicilor și procedurilor interne pe baza informațiilor rezultate din raportul de audit;
3. Elaborarea LIA/DPIA, dacă va fi cazul, în urma auditului;
4. Elaborarea planului de instruire anuală a angajaților;
5. Actualizarea registrului de prelucrare;
6. Instruirea angajaților conform planului anual.

DPO-ul

Responsabilul cu Protecția Datelor – Data Protection Officer, cunoscut în practică și sub acronimul DPO, este persoana desemnată de operatorul de date cu caracter personal care are atribuții în domeniul prelucrării de date efectuate de acesta din urmă.

Desemnarea DPO-ului trebuie privită ca o garanție pentru respectarea planului de conformitate aplicat de companie. De cele mai multe ori, în practică, DPO-ul este numit formal, nefiind instruit și necunoscând practica ori particularitățile companiei în materie de procese de prelucrări interne de date. Multe companii consideră în mod eronat că simpla numire a unui responsabil și notificarea lui la autoritate reprezintă o conformare la cerințele legale aplicabile și chiar o garanție că în eventualitatea unui control nu vor fi aplicate sancțiuni. Or, este evident că nu s-ar mai ridica problema unui plan complex de conformare dacă lucrurile ar fi atât de simple. Problema conformării este mult mai amplă iar compania va avea în vedere un întreg proces și nu doar o numire formală a unei persoane. Din aceeași perspectivă trebuie privită și relația cu un DPO extern. Chiar dacă nu este un salariat al companiei, DPO-ul extern va participa la multiple procese interne astfel încât să se familiarizeze cu specificul activității, funcționând ca un membru al echipei. Este esențial ca responsabilul să cunoască activitatea fiecărui departament intern astfel încât să poată ajuta la conformarea organizației.

GDPR prevede anumite categorii de operatori și persoane împuternicite de operatori care au obligația desemnării unui responsabil cu protecția datelor. Chiar și în cazul în care activitatea desfășurată nu impune numirea unui DPO, recomandarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal este să fie avută în vedere o persoană cu atribuții specifice în acest sens, încurajând efortul voluntar în rândul operatorilor și persoanelor împuternicite de operator.

Funcția de DPO poate fi ocupată de către o persoană din cadrul instituției sau întreprinderii sau se poate externaliza prin intermediul unui contract de prestări servicii. În cazul în care avem în vedere o persoană care este deja salariată a operatorului de date, trebuie evitat conflictul de interese între funcția pe care aceasta deja o ocupă și cea de DPO, interesul fiind acela de a proteja pe cât posibil compania de eventuale decizii greșite ale DPO.

O atenție sporită din partea companiilor trebuie acordată în situația în care este obligatorie numirea unui DPO, existând deja la nivelul Uniunii Europene sancțiuni aplicate pentru neîndeplinirea acestei obligații¹⁵.

Deoarece în prezent există, la nivelul multor companii, opinia conform căreia odată numit un DPO, acesta va duce la îndeplinire orice aspect legat de implementare și va răspunde pentru orice problemă derivată din segmentul protecția datelor, vom stabili, în cele ce urmează, acțiunile în care DPO-ul trebuie implicat pentru aviz sau consultare și sarcinile pe care DPO-ul trebuie să le îndeplinească.

! ● **Exemplu:** Pentru întocmirea DPIA, DPO-ul trebuie implicat pentru aviz. Așadar, nu DPO-ul este persoana care redactează acest document. DPIA trebuie privită ca un proiect în care managementul este direct implicat împreună cu alți specialiști, fiind necesar avizul DPO cu privire la necesitatea întocmirii documentului, metodologia utilizată, strategia pentru reducerea eventualelor riscuri asupra drepturilor și intereselor persoanelor vizate precum și pentru verificarea finală a evaluării de impact.

Solicitarea avizului DPO-ului la efectuarea evaluării de impact relevă importanța calității sale, fiind foarte important ca acesta să fie considerat un partener de discuții în cadrul organizației și să fie consultat în orice operațiune ce implică aspecte de protecție a datelor cu caracter personal.

! ● **Exemplu:** Operatorul păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor. Așadar, nu DPO-ul este persoana responsabilă pentru întocmirea registrului, aceasta rămânând o obligație în sarcina companiei, indiferent dacă DPO-ul este intern sau s-a optat pentru externalizare.

Cel mai important rol pe care DPO-ul și după caz, echipa pe care acesta o coordonează și-l asumă este implicarea, pe cât posibil, în toate aspectele legate de protecția datelor în cadrul tuturor departamentelor interne.

¹⁵ Germania – The Federal Commissioner for Data Protection and Freedom of Information a aplicat, în anul 2019, o amendă de 10.000 de euro pentru lipsa desemnării unui DPO;

Austria – Austrian Data Protection Authority a aplicat, în anul 2019, o amendă de 50.000 de euro pentru lipsa desemnării unui DPO;

Germania – Data Protection Authority of Hamburg a aplicat, în anul 2019, o amendă de 51.000 de euro pentru numirea necorespunzătoare a unui DPO.

GDPR trasează o serie de sarcini DPO-ului, aliniate cu independența conferită de acest statut. În linii mari, DPO-ul informează și consiliază compania și angajații care se ocupă de prelucrare cu privire la obligațiile legale privind protecția datelor, monitorizează respectarea cadrului legal aplicabil și a politicilor interne ce asigură conformitatea companiei, se implică așa cum am arătat, în elaborarea și monitorizarea DPIA și cooperează cu A.N.S.P.D.C.P., asumându-și rolul de punct de contact.

Pentru a da eficiență rolului pe care responsabilul îl are, compania ar trebui să se asigure ca DPO-ul să fie invitat la discuții ale conducerii, să i se solicite avizul în cazul în care se iau decizii cu implicații directe asupra protecției datelor și că se ține cont de acest aviz, recomandându-se ca în cazurile în care există un dezacord între DPO și conducere să fie efectuată o documentare a motivelor pentru care nu se respectă avizul.

În ceea ce privește pregătirea profesională, GDPR nu impune o calificare specifică, ci doar cunoștințe de specialitate în domeniul protecției datelor cu caracter personal. Pentru pregătirea profesională a DPO-ului se pot avea în vedere cursuri, conferințe, workshop-uri dedicate și instruirii în materie. Numirea unui DPO presupune pentru companie alocarea unui buget, în vederea menținerii și îmbunătățirii cunoștințelor în materie de protecția datelor.

La nivel național, Autoritatea Națională pentru Calificări a aprobat Standardul ocupațional pentru Responsabil cu Protecția Datelor (COR 242231). Furnizorii de formare profesională autorizați organizează, în prezent, sesiuni de instruire teoretică și practică urmând tematica acestui standard finalizate prin susținerea unui examen organizat de formator împreună cu Autoritatea Națională pentru Calificări.

Evidența activităților de prelucrare

Obligația de a păstra evidența activităților de prelucrare (cunoscută în practică și ca registrul de prelucrări de date ori ca maparea prelucrărilor de date – „data mapping”) poate fi aplicabilă atât pentru operatori, cât și pentru împuterniciți. Registrul activităților de prelucrare poate fi conceput atât în formă scrisă, pe suport de hârtie, cât și în formă electronică. Adițional utilizării pachetului MS Office, de exemplu, se pot utiliza și programe special dedicate în acest sens, acolo unde acest lucru este posibil. În practică au fost dezvoltate multiple mecanisme care să permită întocmirea evidenței.

Exemplu: în acordul de prelucrare încheiat între operator și împuternicit este prevăzut faptul că împuternicitul va păstra o evidență a proceselor de prelucrări de date rezultate din derularea relației contractuale între cele două părți. În acest scop, împuternicitul apelează la o platformă dedicată care permite generarea registrului de prelucrări la care primește acces și operatorul pe bază de user și parolă.

Când această obligație este aplicabilă sau chiar și în ipoteza în care operatorul ori împuternicitul în mod voluntar optează pentru păstrarea acestui document ca măsură organizatorică menită să demonstreze conformitatea, vor fi avute în vedere dispozițiile Regulamentului în materie de evidențe ale prelucrărilor de date. Conform art. 30 GDPR, documentul va conține numele și prenumele operatorului și ale DPO-ului, scopurile prelucrărilor, o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal prelucrate, categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări sau organizații internaționale, dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și a eventualelor documente ce demonstrează implementarea unor garanții adecvate și acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate implementate.

Avantajul păstrării registrului de prelucrare de date poate fi privit din mai multe perspective:

- din punct de vedere legal: îndeplinirea unei obligații legale (documentează elementele obligatorii prevăzute de GDPR);
- din punct de vedere practic: contribuie la identificarea elementelor cheie ale prelucrării datelor cu caracter personal și sprijină DPO-ul și compania în administrarea procesului de prelucrare a datelor cu caracter personal.

Definirea activităților de prelucrare

Din punct de vedere al activităților de prelucrare, se vor identifica principalele activități avându-se, desigur în vedere faptul că în cele mai multe cazuri, acestea se efectuează concomitent:

- Colectare (activitatea de prelucrare va avea în vedere atât colectare prin intermediul documentelor scrise – contracte, formulare etc., dar și

online – vizitare site, aplicare pentru un post vacant disponibil prin intermediul unui formular dedicat etc.);

- Înregistrare (activitatea de prelucrare va avea în vedere înregistrarea pe suport hârtie dar și în sisteme IT);

- Structurare și organizare (activitatea de prelucrare va avea în vedere transformarea datelor cu caracter personal în vederea unei mai bune gestionări);

- Stocare (activitatea de prelucrare va avea în vedere salvarea datelor cu caracter personal. Aceasta se poate realiza prin intermediul unei sau a mai multor baze de date. Compania nu se va limita la stocare în evidențe electronice, luând în calcul și arhivarea documentelor pe format hârtie);

- Adaptare sau modificare (activitatea de prelucrare va avea în vedere efectuarea unor modificări la nivelul unui set de date cu caracter personal – EXEMPLU: modificarea datelor unui salariat care și-a schimbat cartea de identitate în evidențele angajatorului sau modificarea adresei unui client existent în baza de date);

- Extragere (activitatea de prelucrare va avea în vedere extragerea unui set de date în vederea prelucrării ulterioare);

- Consultarea și utilizarea (activitatea de prelucrare va avea în vedere consultarea propriu-zisă, mai exact vizualizarea datelor personale. Implicit, acțiunea de vizualizare presupune și o utilizare a datelor în cauză);

- Divulgarea și diseminarea (activitatea de prelucrare va avea în vedere trimiterea sau expedierea datelor către o terță persoană/entitate);

- Restricționare (activitatea de prelucrare poate viza blocarea accesului, respectiv a posibilității de vizualizare a datelor cu caracter personal);

- Ștergere sau distrugere (activitatea de prelucrare va avea în vedere atât mediile IT de stocare cât și cele de stocare fizică a materialelor tipărite);

- Alinierea sau combinarea (activitatea de prelucrare va avea în vedere centralizarea datelor similare din mai multe surse).

Etapele de implementare ale registrului de prelucrare

Elaborarea unui registru de prelucrare care să descrie în detaliu activitățile de prelucrare, astfel încât acest document să reprezinte o „oglindă” a proceselor de prelucrare derulate la nivel de companie presupune respectarea unor etape graduale care au ca scop final

consolidarea unui registru care prezintă fidel elementele prevăzute de GDPR:

- **Conștientizarea** asupra necesității implementării acestei măsuri organizatorice: acest pas presupune informarea departamentelor interne privind existența cerințelor legale și a bunelor practici pe care compania dorește să le implementeze. Managementul organizației, împreună cu DPO-ul pot conlucra în vederea bifării acestui prim pas, pornind de la un training intern în cadrul căruia se poate prezenta inclusiv planul de conformare care cuprinde și acest element;

- **Informare:** acest pas presupune familiarizarea coordonatorilor departamentelor cu etapele de urmat în materie de implementare a evidenței de prelucrare a datelor. Managementul organizației, împreună cu DPO-ul pot organiza training-uri, workshop-uri, sesiuni de FAQ pe acest subiect pentru identificarea în detaliu a proceselor de prelucrare specifice fiecărui departament;

- **Interogare:** acest pas implică, de asemenea, un proces de conlucrare între management, DPO și reprezentanții departamentelor (de exemplu, HR, Financiar-Contabilitate, Juridic, Marketing, Achiziții, Vânzări etc.) care are drept obiectiv final identificarea tuturor detaliilor de țin de prelucrarea datelor cu caracter personal. Chestionarele pot fi chiar cele avute în vedere pentru auditul inițial sau periodic. Urmare a comunicării chestionarelor de interogare către reprezentanți, salariații care activează în cadrul departamentului respectiv vor oferi detaliile necesare elaborării registrului de prelucrare;

- **Consultare:** acest pas implică disponibilitatea managementului și a DPO-ului, în vederea sprijinirii departamentelor interne în vederea clarificării eventualelor neclarități ori nelămuriri ce ar putea rezulta din chestionarele de interogare. În acest sens, pot fi stabilite ședințe periodice care să monitorizeze acest proces la nivelul fiecărui departament;

- **Consolidare și implementare:** acest pas final presupune structurarea tuturor informațiilor comunicate de către departamente. Într-o primă etapă, se va verifica corectitudinea informațiilor furnizate, DPO-ul având un rol esențial în acest punct. Ulterior, fiecare proces de prelucrare va fi transpus în evidența activităților de prelucrare. La finalizarea registrului de prelucrare, se va solicita o validare finală din partea coordonatorilor departamentelor;

- **Actualizare:** acest pas trebuie privit ca un proces continuu. În funcție de necesitățile companiei și de apariția unor procese de prelucrare noi, registrul va fi actualizat în mod corespunzător.

! • **Exemplu:** o companie care lucrează în domeniul marketing dorește să integreze o nouă linie de business în materie de recrutare personal. Având în vedere deosebirile majore între vechea activitate de bază și noua direcție de business, este clar că trebuie urmat întregul proces pentru evidența activităților de prelucrare inclusiv pentru acest segment.

Ca bună practică, se recomandă validarea periodică a registrului de prelucrare, chiar dacă procesele interne de prelucrări nu suferă modificări care să impună o ajustare a registrului de prelucrare.

Unul dintre cei mai importanți pași din cei menționați mai sus este interogarea proceselor de prelucrare, unde este foarte importantă implicarea departamentelor interne, deoarece informațiile livrate ca urmare a interogării reprezintă conținutul fundamental al registrului privind prelucrările de date cu caracter personal.

Elementele registrului de prelucrare

- Nume și date de contact: se vor documenta denumirile și datele de contact ale operatorului de date, persoanele împuternicite, DPO și a reprezentanților operatorului din țări terțe;

- Scopurile prelucrării – de exemplu: plata salariilor, înregistrări în REVISAL, plata contribuțiilor, organizarea de evenimente interne, stabilirea unor parteneriate business-to-business, achiziția de mărfuri, supravegherea spațiilor prin intermediul unor mijloace de supraveghere video, înregistrarea vizitatorilor, măsurarea temperaturii corporale etc.

- Activitățile de prelucrare: se vor menționa activitățile de prelucrare detaliate mai sus prin raportare la scopurile identificate;

- Categoriile de persoane vizate și tipurile de date cu caracter personal: vor fi identificate persoanele vizate din interiorul companiei și din afara acesteia care fac obiectul prelucrărilor de date cu caracter personal dar și datele prelucrate cu privire la aceste persoane;

!

Exemplu:

- persoane vizate angajați ai societății/aplicanți pentru un loc de muncă: date din dosarul de personal: datele din cartea de identitate, permis de ședere, permis de muncă etc, datele din pontaje

prelucrate prin intermediul cardurilor de acces, locația prelucrată prin intermediul mijloacelor GPS, imaginea prelucrată prin intermediul mijloacelor de supraveghere video, datele privind evaluările profesionale ale angajaților, datele din aplicațiile candidaților pentru un anumit loc de muncă, datele privind membrii de familie etc.;

- persoane vizate care și-au dat acordul în scopuri de marketing: adresa de e-mail pentru transmiterea de newslettere săptămânale, numărul de telefon al persoanelor care au optat pentru informări prin intermediul acestui canal etc.;
- persoane vizate clienți sau persoane vizate reprezentanți ai clienților persoane juridice: date necesare facturării: nume, prenume, adresă domiciliu, date necesare prelucrării comenzii: număr de telefon, adresă de livrare etc, date privind istoricul plăților, date privind istoricul comenzilor etc.;
- Categoriile de destinatari: vor fi identificate entitățile către care se comunică date cu caracter personal prin raportare la procesele de prelucrare specifice persoanelor vizate.



Exemplu:

- Datele angajaților vor fi transmise către ANAF, asigurători sociali, firme de asigurare, societăți care prestează serviciile de medicină muncii, dar și către alte departamente ale societății (Financiar-Contabilitate, Juridic etc.);
- Datele pentru activități de marketing vor fi transmise agenției de publicitate cu care se colaborează;
- Transferul în țări terțe: vor fi identificate și detaliate entitățile către care se transmit date personale din afara Spațiului Economic European. De asemenea, în cazul în care sunt identificate și înregistrate în evidență astfel de transferuri, vor fi identificate și măsurile aferente de protecție a datelor cu caracter personal, în funcție de localizarea geografică a țării din care provine entitatea destinatară.

Măsuri tehnice și organizatorice: vor fi identificate și descrise succint măsurile implementate pentru asigurarea confidențialității și securității datelor cu caracter personal.

Evaluarea impactului asupra protecției datelor

Evaluarea impactului asupra protecției datelor, cunoscută în practică și sub acronimul DPIA (Data Protection Impact Assessment) sau sub

denumirea de studiu de impact, permite companiei să analizeze în concret modul în care implementarea unui proces, a unui proiect sau sistem poate aduce atingere drepturilor persoanelor vizate.

Obiectivul DPIA constă în analiza detaliată a procesului/proceselor de prelucrare, în evaluarea necesității și proporționalității prelucrării, în identificarea eventualelor riscuri ce ar putea rezulta din activitatea de prelucrare în raport cu drepturile și libertățile persoanelor vizate precum și a metodelor de gestionare în sensul stabilirii de măsuri care să le atenueze sau după caz, să le elimine. Cu alte cuvinte, acest instrument are rolul de a identifica și reduce sau după caz, elimina, riscurile rezultate din eventuala pierdere a confidențialității datelor persoanelor vizate.

Din perspectiva responsabilității operatorului, DPIA are rolul de a demonstra conformitatea, nu doar în relația cu autoritatea de supraveghere, ci și în relația cu terții, DPIA putând fi o cerință esențială în evaluările partenerilor pe care le realizează anumiți operatori în contextul demarării unor negocieri în vederea încheierii unui contract.

Responsabilitatea privind întocmirea DPIA aparține companiei, însă va fi implicat și DPO-ul în vederea avizării evaluării și în măsura în care există la nivel intern, un specialist în securitatea datelor, coordonator al întregii activități dedicate acestui segment. Dacă volumul personalului nu presupune identificarea acestor funcții interne, pentru întocmirea documentului compania poate apela la ajutor specializat extern. În măsura în care există desemnat un DPO intern sau extern care a oferit aviz cu privire la DPIA, acesta va ajuta, în continuarea ciclului de viață al procesului implementat, la monitorizarea DPIA.

În ceea ce privește obligativitatea întocmirii acestui document intern, cerințele GDPR vor fi cumulate cu cele ale Deciziei A.N.S.P.D.C.P. nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.

GDPR impune întocmirea DPIA în cazul în care procesul/procesele de prelucrare sunt susceptibile să genereze un risc ridicat în ceea ce privește drepturile și libertățile persoanelor vizate. Deși obligația legală privind întocmirea unui astfel de document nu se extinde asupra oricărui proces de prelucrare ce poate conduce la riscuri, se recomandă, mai ales în situațiile în care nu se poate stabili nivelul de risc, ca la nivel de companie să existe acest document, privit ca o bună practică în cadrul planului de conformare.

În măsura în care DPIA vizează un proces de prelucrare în care este implicat și un împuternicit, documentul va fi realizat cu ajutorul informațiilor primite de la acesta.

Fără a trata exhaustiv lista situațiilor în care s-ar impune redactarea DPIA, GDPR identifică cazurile în care DPIA este obligatorie. Aceste situații sunt reluate și completate de Decizia A.N.S.P.D.C.P. nr. 174/2018. Este, așadar, obligatoriu să fie întocmită DPIA în toate ipotezele de mai jos:

- în cazul unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

- în cazul prelucrării pe scară largă a unor categorii speciale de date (privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viața sexuală sau orientarea sexuală ale unei persoane fizice) sau a datelor cu caracter personal referitoare la condamnări penale și infracțiuni;

- în cazul unei monitorizări sistematice pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, piețe, parcuri sau alte asemenea spații;

- în cazul prelucrării pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor și ale angajaților, prin mijloace automate de monitorizare și/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfășurării activităților de reclamă, marketing și publicitate;

- în cazul prelucrării pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special, în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-și exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaștere facială în vederea facilitării accesului în diferite spații;

- în cazul prelucrării pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicații „Internetul lucrurilor”, cum ar fi smart TV, vehicule conectate, contouri inteligente, jucării inteligente, orașe inteligente sau alte asemenea aplicații);

- în cazul prelucrării pe scară largă și/sau sistematică a datelor de trafic și/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situații) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

DPIA ar trebui întocmită, pentru asigurarea unui proces eficient și durabil, anterior demarării procesului de prelucrare deși pe parcurs ar putea interveni elemente noi. Faptul că s-ar impune o actualizare DPIA ulterior începerii procesului de prelucrare nu este un motiv valid pentru amânarea sau neaplicarea unei DPIA. Așa cum arată și WP29, DPIA este un proces continuu, nu un exercițiu unic.

Trasarea elementelor la care face referire GDPR cu privire la conținutul DPIA ar putea conduce la ideea conform căreia un astfel de document ar fi de avut în vedere doar pentru companii de dimensiuni mari, însă analizând cerințele legale se poate observa faptul că GDPR stabilește doar un cadru general conturat de o descriere a procesului de prelucrare, o evaluare a proporționalității, identificarea riscurilor și a măsurilor de abordare, astfel încât acestui document i se poate da eficiență doar prin caracteristicile specifice ale organizației, indiferent de dimensiunea pe care aceasta o are.

Ca bună practică, se poate avea în vedere publicarea DPIA sau a unor părți din acest document, aspect ce ar valida atitudinea companiei în responsabilității și transparenței și ar spori încrederea în conformitatea companiei.

Analiza interesului legitim

Analiza interesului legitim, cunoscută în practică și sub acronimul LIA (Legitimate Interest Assessment) este un document intern ce studiază interesul legitim utilizat de o companie ca temei al prelucrării de date.

Interesul legitim este un temei legal des întâlnit în cadrul proceselor de prelucrare identificate la nivelul unei companii. Cerința legală pentru utilizarea acestui temei este ca interesul legitim al companiei să nu prevaleze drepturilor și libertăților fundamentale ale persoanelor vizate.

LIA presupune o testare pe trei segmente:

- identificarea interesului legitim („*purpose test*”/ „*identity test*”);



• **Exemplu:** Aspecte pe care compania ar putea să le trateze în această primă etapă a pregătirii LIA:

1. Care este motivul pentru care se dorește prelucrarea datelor cu caracter personal?
2. Care sunt beneficiile pe care le aduce acest proces de prelucrare companiei?
3. Cât de importante sunt avantajele identificate?

4. Care ar fi impactul asupra companiei dacă s-ar decide să se renunțe la procesul de prelucrare?

5. Sunt/pot fi respectate cerințele specifice pentru protejarea datelor rezultate din procesul de prelucrare? Sunt avute în vedere cerințele legale minime sau sunt avute în vedere și bune practici, ca măsuri suplimentare pentru asigurarea conformității?

- analiza necesității („*necessity test*”);



• **Exemplu:** Aspecte pe care compania ar putea să le abordeze în fundamentarea necesității:

1. Prelucrarea ajută efectiv la atingerea obiectivelor identificate?

2. Prelucrarea este proporțională cu obiectivele?

3. Există vreo modalitate de a atinge aceleași obiective fără acest proces de prelucrare?

4. Se pot atinge aceleași obiective minimizând datele rezultate din procesul de prelucrare?

5. Se pot atinge aceleași obiective apelând la metode care să afecteze într-o măsură mai redusă dreptul la viață privată al persoanelor vizate?

- analiza proporționalității („*proportionality test*”);



• **Exemplu:** Aspecte pe care compania ar putea să le abordeze în fundamentarea proporționalității:

1. Există o relație relevantă între companie și persoanele vizate? Care este natura relației?

2. În ce scop au fost colectate datele personale? În urmă cu cât timp?

3. Persoana vizată se poate aștepta la prelucrarea datelor în vederea atingerii obiectivelor companiei?

4. Există suficiente garanții pentru atenuarea impactului generat de procesul de prelucrare?

LIA reprezintă un tip de evaluare sumară a riscului generat de un proces de prelucrare realizat în interesul legitim al companiei. În măsura în care analiza proporționalității ar identifica segmente pentru care este necesară o fundamentare riguroasă, se recomandă ca organizația să aibă în vedere elaborarea unei DPIA.

Instruirea salariaților

În cadrul procesului de conformare, compania trebuie să se asigure de eficiența planului implementat. Practica actuală a autorităților de

supraveghere ne arată faptul că securitatea datelor a fost afectată de cele mai multe ori urmare a erorilor umane și nu a unor atacuri informatice.

În cadrul proceselor de implementare, factorul uman apare ca fiind elementul vulnerabil în asigurarea conformității. Atunci când personalul nu cunoaște cerințele legale și planul de conformare al companiei precum și riscurile ce derivă din nerespectarea acestora, putem asista la incidente de securitate.

Companiile trebuie să conștientizeze faptul că o implementare cunoscută doar la nivel de management și eventual, la nivelul DPO-ului desemnat nu asigură conformitatea proceselor de prelucrare.

Rolul instruirii salariaților este de a responsabiliza factorul uman care intră în contact cu datele personale, fie ale clienților, fie ale colegilor, indiferent de departamentul în care activează. Responsabilizarea angajaților demonstrează aplicarea conceptelor *privacy by design* și *privacy by default*, prin adoptarea unei atitudini proactive din partea companiei, în scopul preîntâmpinării apariției incidentelor de securitate.

Instruirea salariaților ar trebui gândită în funcție de o serie de factori, precum dimensiunea organizației, complexitatea proceselor de prelucrare, specificul activității etc.



● **Exemplu:** La nivelul unei organizații de dimensiuni reduse, cu procese de prelucrare ce nu implică date sensibile, se va avea în vedere o instruire de bază, fără a intra în detalii ce nu sunt aplicabile activității desfășurate.

Tematica unei astfel de instruirii ar putea viza următoarele elemente:

1. Ce sunt datele cu caracter personal? Exemple de categorii de date cu caracter personal.
2. Ce este GDPR? Descriere generală a legislației aplicabile.
3. Ce documente privind protecția datelor sunt implementate la nivelul organizației?
4. Măsurile tehnice și organizatorice implementate.
5. Obligațiile angajaților privind protecția datelor cu caracter personal.
6. Consecințele nerespectării legislației aplicabile și a documentelor interne implementate.



● **Exemplu:** La nivelul unei organizații cu peste 500 angajați se poate avea în vedere o instruire specifică organizată la nivelul fiecărui departament.

Tematica unei astfel de instruiți ar putea viza, în ceea ce privește Departamentul de Resurse Umane, următoarele elemente:

1. Ce date cu caracter personal sunt prelucrate în vederea derulării relației de muncă? Importanța monitorizării fluxului de date și actualizarea Politicii privind datele cu caracter personal a Departamentului de Resurse Umane.

2. Ce date cu caracter personal sunt prelucrate în cadrul proceselor de recrutare? Importanța monitorizării fluxului de date și actualizarea Politicii privind datele cu caracter personal a Departamentului de Resurse Umane.

3. Respectarea principiului limitării accesului la date – însușirea procedurii interne privind accesul la datele salariaților.

4. Respectarea măsurilor tehnice și organizatorice din Politica privind datele cu caracter personal a Departamentului de Resurse Umane.

5. Divulgarea datelor salariaților către alte departamente din companie – însușirea procedurii interne privind divulgarea datelor din Departamentul de Resurse Umane.

6. Consultarea DPO în vederea implementării unor mijloace tehnice ce presupun prelucrarea datelor salariaților.

! **Exemplu:** În ceea ce privește Departamentul Marketing, instruirea ar putea viza următoarea tematică:

1. Datele cu caracter personal prelucrate în cadrul Departamentului Marketing. Stabilirea proceselor de prelucrare – inclusiv mediul online și concursuri.

2. Analiza contractelor încheiate cu agențiile de publicitate prin raportare la specificul colaborării.

3. Respectarea principiului limitării accesului la date – însușirea procedurii interne privind accesul la datele de marketing (acces limitat pentru datele colectate din mediul online, acces limitat pentru datele colectate în vederea derulării concursurilor).

4. Respectarea măsurilor tehnice și organizatorice din Politica privind datele cu caracter personal a Departamentului Marketing.

5. Divulgarea datelor câștigătorilor anumitor campanii/concursuri către Departamentul Financiar – însușirea procedurii interne privind divulgarea datelor din cadrul Departamentului Marketing.

6. Informarea DPO în cazul extinderii activităților de marketing.

! ● **Exemplu:** În ceea ce privește Departamentul Securitate, instruirea ar putea viza următoarea tematică:

1. Datele cu caracter personal prelucrate în cadrul Departamentului Securitate. Importanța datelor colectate prin intermediul mijloacelor video și de geolocalizare.

2. Informarea persoanelor vizate cu privire la procesele de prelucrare prin intermediul mijloacelor video și de geolocalizare. Măsuri tehnice și organizatorice implementate și revizuirea periodică a acestora.

3. Divulgarea datelor prelucrate în cadrul Departamentului Securitate către alte departamente din companie și către organele abilitate – însușirea procedurii privind divulgarea datelor din cadrul Departamentului Securitate.

4. Consultarea DPO pentru orice activitate suplimentară sau mijloc nou utilizat în cadrul Departamentului Securitate.

! ● **Exemplu:** La nivelul unei clinici medicale se va avea în vedere o instruire complexă, prin raportare la procesele interne ce implică prelucrarea de date (inclusiv sensibile). Tematica urmărită ar putea avea în vedere:

1. Ce sunt datele cu caracter personal? Exemple de categorii de date cu caracter personal. Datele medicale cu privire la pacienți – încadrare.

2. Ce este GDPR? Descriere generală a legislației aplicabile.

3. Ce documente privind protecția datelor sunt implementate la nivelul clinicii medicale?

4. Datele cu caracter personal prelucrate în vederea unei programări. Documente completate de pacient. Programarea efectuată prin intermediul site-ului.

5. Datele cu caracter personal din dosarul pacientului. Prelucrarea prin intermediul aplicațiilor specifice.

6. Măsuri tehnice și organizatorice implementate.

7. Utilizarea datelor pacienților în scopuri de marketing.

8. Informarea DPO-ului cu privire la solicitările pacienților în legătură cu datele cu caracter personal – acțiunile personalului care primește solicitări din partea persoanelor vizate.

9. Incidentele de securitate. Riscuri. Responsabilitățile personalului în cazul în care intervine un incident de securitate. Investigarea incidentului și notificarea A.N.S.P.D.C.P..

O abordare similară poate fi avută în vedere și în cazul companiilor ce desfășoară activități în domeniul fitness și nutriție ori în cazul școlilor și grădinițelor, situație în care se va acorda o atenție sporită, dată fiind prelucrarea datelor unei categorii speciale de persoane vizate – persoane vulnerabile (minori).

Materialele pe care compania le va pune la dispoziția angajaților se pot prezenta sub mai multe forme: prezentări, materiale video, infografice, broșuri etc.

Instruirea se poate finaliza cu un test, fie scris, fie organizat ca un dialog având ca obiectiv verificarea cunoștințelor dobândite de către angajați.

Ca bună practică, se recomandă ca planul de instruire pentru angajați să cuprindă, pe lângă un minimum de 2-3 sesiuni de instruire anuală și o verificare periodică a cunoștințelor personalului, în special pe segmentele în care riscurile privind producerea incidentelor de securitate sunt mai ridicate. Acolo unde procesele de prelucrare impun o departajare a instruirii la nivel de departamente, compania va avea în vedere un număr optim de instruiți la nivelul fiecărui departament.

Dovada instruirii se face, de regulă, cu procesul-verbal privind instruirea angajaților întocmit la finalizarea programului de instruire. Un astfel de document ar putea cuprinde tematica training-ului/instruirii/reinstruirii, data, numărul participanților, numele persoanei care realizează instruirea (trainer/formator), locul în care acesta este efectuat, concluziile în urma testării scrise sau după caz, a dialogului de verificare și eventualele observații ale participanților. De cele mai multe ori, DPO este persoana responsabilă atât pentru întocmirea planului anual de instruire, cât și pentru instruirea efectivă a angajaților, în funcție de necesitățile companiei.

O sesiune de instruire poate fi un bun prilej în care compania informează angajații cu privire la datele personale pe care le prelucrează în derularea relației de muncă sau după caz, în care reia informarea acestora cu privire la prelucrarea datelor de către angajator.

Compania nu ar trebui să se concentreze exclusiv pe datele personale ale persoanelor vizate care interacționează cu organizația în vederea derulării de relații comerciale și să acorde o importanță redusă persoanelor vizate, angajați ai societății. Ca orice altă persoană vizată, angajatul are toate drepturile prevăzute de legislație cu privire la datele personale pe care angajatorul le prelucrează, iar compania, la rândul său, are față de angajați toate obligațiile pe care le are față de celelalte persoane vizate.

Limitarea accesului

Limitarea accesului presupune, pe de o parte, implementarea unor măsuri de securitate fizică pentru protecția spațiilor în care se prelucrează datele cu caracter personal, iar pe de altă parte, limitarea accesului prin trasarea clară de către management, a atribuțiilor și responsabilităților fiecărui salariat în ceea ce privește gestionarea datelor cu caracter personal pentru îndeplinirea atribuțiilor de serviciu.

În ceea ce privește măsurile de securitate fizică pentru protecția spațiilor în care se prelucrează date cu caracter personal, compania poate avea în vedere atât un control clasic, pe bază de cheie păstrată de unul sau mai mulți responsabili, cât și un control pe bază de coduri de acces sau alte mijloace similare moderne. Pentru un control cât mai eficient, se poate opta pentru păstrarea unei liste cu persoanele care sunt autorizate în vederea accesului în spațiile în care sunt prelucrate date cu caracter personal, fie că se are în vedere păstrarea documentelor pe suport hârtie, fie echipamentele IT. Suplimentar, ca bună practică, se poate avea în vedere și păstrarea unui registru de acces în spațiile dedicate păstrării documentelor arhivate sau în incintele în care sunt echipamentele IT.

În completarea măsurilor pentru limitarea accesului în spațiile în care sunt prelucrate date cu caracter personal, compania va avea în vedere instituirea unor reguli clare de securitate IT în rândul angajaților pentru stațiile de lucru sau orice alt echipament utilizat în activitatea curentă.



● **Exemplu:** Politica de Securitate IT a companiei prevede cerințe de securitate pentru stațiile de lucru, incluzând aspecte privind setarea parolei urmând anumite reguli precise și modificarea la anumite intervale de timp urmând aceleași reguli, privind blocarea stației de lucru în momentul părăsirii biroului, referitoare la transferul intern de informații etc.

Permiterea accesului doar la datele cu caracter personal de care angajatul are nevoie în vederea îndeplinirii atribuțiilor ar putea presupune o stabilire, la nivel intern, a drepturilor de acces în funcție de specificul atribuțiilor pe care un salariat le are în cadrul raportului de muncă.



● **Exemplu:** La nivelul organizației, drepturile de acces se acordă în baza solicitării coordonatorului de departament. Astfel, când un nou salariat care va lucra pe segmentul de recrutare își începe activitatea

în cadrul Departamentului Resurse Umane, Directorul de Resurse Umane solicita acces de la Departamentul IT doar pentru baza de date de CV-uri și alte documente necesare procesului de recrutare.

Limitarea accesului ar putea presupune ca organizația să fie preocupată să instituie reguli în vederea interzicerii partajării conturilor ce permit accesul la date, să evite acordarea accesului la mai multe categorii de date decât este necesar pentru îndeplinirea atribuțiilor trasate în fișa postului sau să dispună retragerea dreptului de acces odată ce raporturile de muncă pe baza cărora s-a realizat accesul la date încetează.

Politici și proceduri

În funcție de particularitățile pe care le prezintă activitatea desfășurată de companii, acestea implementează politici și proceduri interne privind protecția datelor cu caracter personal.

Nu există un standard, un model precis de urmat în elaborarea acestor documente, urmând ca fiecare organizație să gândească politicile și procedurile ca un instrument eficient menit să asigure îndeplinirea obligațiilor impuse de GDPR.

În practică, există multiple abordări asupra politicilor și procedurilor interne privind protecția datelor. Unele companii au decis implementarea unui set de proceduri generale aplicabile unitar în companie, altele au abordat politici specifice fiecărui departament.

Indiferent însă de multitudinea documentelor existente la nivel intern, în analiza conformității se urmărește dacă regulile inserate în aceste documente sunt în mod real aplicate.

Cea mai mare problemă pe care o putem identifica în prezent, în rândul companiilor care au implementat astfel de politici și proceduri, este legată de faptul că documentele de implementare există la nivel intern fără a fi însă realmente puse în aplicare. Mai mult decât atât, sunt companii în cadrul cărora angajații nici nu cunosc planul de conformare și nici existența unor astfel de politici și proceduri ce reglementează intern acest segment. Se creează, așadar, doar o aparență de drept în timp ce o multitudine de riscuri pot exista în continuare în ceea ce privește eventualele incidente de securitate.

Se recomandă ca, în urma unui audit preliminar, în funcțiile de probleme identificate, să se stabilească politicile și procedurile ce urmează a fi aplicate, în funcție de o serie de factori interni precum numărul de salariați, abordarea salariaților, volumul de documente interne deja

existent etc. Pentru ca implementarea politicilor și procedurilor să fie una eficientă, compania poate opta pentru includerea etapizată a documentelor GDPR în plan intern. Aceste decizii țin, în mare parte de cultura organizațională și de aceea este foarte importantă implicarea managementului.



● **Exemplu:** La nivelul unei companii ce desfășoară activitate în domeniul cursurilor de instruire pentru copii, se pot avea în vedere următoarele politici și proceduri interne, în completarea celorlalte documente avute în vedere în procesul de conformare:

1. Politica privind gestionarea datelor cu caracter personal prelucrate la nivelul companiei; Datele persoanelor vulnerabile – precauții;
2. Politica privind exercitarea drepturilor persoanelor vizate;
3. Politica privind rețenția datelor;
4. Politica de securitate IT;
5. Politica privind incidentele de securitate;
6. Procedura privind elaborarea analizelor intereselor legitime (LIA) și evaluărilor de impact (DPIA);
7. Procedura privind întocmirea și actualizarea registrului de prelucrare;
8. Procedura de lucru cu DPO-ul desemnat;



● **Exemplu:** La nivelul unei companii ce desfășoară activitate în domeniul stomatologiei se pot avea în vedere următoarele politici și proceduri interne, în completarea celorlalte documente avute în vedere în procesul de conformare:

1. Politica privind gestionarea datelor pacienților de către personalul auxiliar (programări și activități de recepție).
2. Politica privind gestionarea datelor pacienților de către medicii stomatologi;
3. Politica de acces intern la datele pacienților;
4. Procedura de clasificare a documentelor interne;
4. Politica privind rețenția datelor;
5. Politica de securitate fizică;
6. Politica privind mijloacele de supraveghere video;
8. Politica privind exercitarea drepturilor persoanelor vizate;
9. Politica privind incidentele de securitate;
10. Politica de marketing;
11. Procedura privind transferul datelor pacienților către terți;

12. Procedura privind elaborarea analizelor intereselor legitime (LIA) și evaluărilor de impact (DPIA);

13. Procedura privind întocmirea și actualizarea registrului de prelucrare.



● **Exemplu:** La nivelul unei companii ce desfășoară activitate în domeniul producției de produse alimentare, se pot avea în vedere următoarele politici și proceduri interne, în completarea celorlalte documente avute în vedere în procesul de conformare:

1. Politica privind protecția datelor pentru Departamentul de Resurse Umane;

2. Procedura privind recrutarea;

3. Procedura privind prelucrarea datelor din dosarele de salariat;

4. Măsurile de securitate implementate la nivelul departamentului de Resurse Umane;

5. Procedura privind transferul intern de date – de la Departamentul Resurse Umane către alte departamente;

6. Politica privind protecția datelor pentru Departamentul Marketing;

7. Procedura pentru campanii on-line;

8. Procedura pentru concursuri și alte campanii off-line;

9. Procedura privind transferul intern de date – de la Departamentul de Marketing către alte departamente;

10. Politica privind protecția datelor în cadrul Departamentului Vânzări;

11. Procedura privind încheierea contractelor;

12. Procedura privind cardurile de fidelitate;

13. Procedura privind transferul intern de date – de la Departamentul Vânzări către alte departamente;

14. Politica privind protecția datelor în cadrul Departamentului Financiar;

15. Procedura privind transferul de date – de la Departamentul Financiar către alte departamente și către autoritățile ce implică activitatea departamentului;

16. Politica privind accesul intern la datele companiei;

17. Politica privind telemunca;

18. Politica privind protecția datelor în cadrul Departamentului IT;

19. Politica privind flota auto;

20. Politica privind mijloacele de supraveghere video;

21. Procedura de lucru cu DPO.



Exemplu: La nivelul unei companii ce desfășoară activitate în domeniul de furnizare servicii internet (de tipul free WiFi pentru persoanele vizate în anumite locații), se pot avea în vedere următoarele politici și proceduri interne, în completarea celorlalte documente avute în vedere în procesul de conformare:

1. Politica privind gestionarea datelor prelucrate;
2. Politica de marketing;
3. Procedura privind exercitarea drepturilor persoanelor vizate prin intermediul portalului dedicat;
4. Politica privind securitatea datelor;
5. Politica privind breșele de securitate;
6. Procedura privind analizele interesului legitim (LIA), analizele de securitate (PIA), evaluările de impact (DPIA) și privind actualizarea registrului de prelucrare.

În cele ce urmează vom trata, exemplificativ, o serie de elemente ce s-ar putea regăsi în conținutul politicilor și procedurilor interne.

Politica privind exercitarea drepturilor persoanelor vizate

Un astfel de document ar putea trata toate drepturile prevăzute de GDPR pentru persoanele vizate și exercitarea propriu-zisă a acestora, de la momentul solicitării persoanei vizate și până la finalizarea operațiunii.

Dreptul de acces la date¹⁶

Dreptul de acces la date (ce implică obligația companiei de a furniza datele cu caracter personal ale persoanei vizate: „Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și în caz afirmativ, acces la datele respective” și la o serie de alte informații) trebuie tratat de la momentul colectării datelor, pe toată durata prelucrării datelor și până la momentul solicitării persoanei vizate.

Ca bună practică, la nivelul companiilor se poate avea în vedere simplificarea procedurii pentru exercitarea drepturilor de către salariați, care pot transmite solicitarea către Departamentul de Resurse Umane sau

¹⁶ Articolul 15 GDPR.

către conducere astfel încât acestei categorii de persoane vizate să se ofere acces la date într-o modalitate simplificată.

Dreptul de acces este exercitat cu precădere în practică, fiind necesar ca organizația să fie pregătită pentru oferirea unui răspuns în timp util la o solicitarea în această direcție.

Exercitarea acestui drept poate fi avută în vedere etapizat, după cum urmează:



Exemplu:

Etapă 1: După primirea solicitării, compania verifică dacă prelucrează datele persoanei vizate. În cazul unui răspuns negativ, operatorul explică situația solicitantului, solicitarea putând fi închisă fără a se parcurge următoarele etape.

Etapă 2: Dacă răspunsul este unul pozitiv, operatorul identifică toate procesele de prelucrare interne și dacă este cazul, operatorii și/sau împuterniciții implicați și oferă un raport privind categoriile de date prelucrate și toate procesele în care sunt implicate datele, categoriile de destinatari la care ajung datele persoanei vizate, aspecte privind durata de retenție, informații despre sursa datelor și dacă este cazul, aspecte privind transferul internațional al datelor.

Regula generală impusă de GDPR cu privire la timpul de răspuns la solicitarea persoanei vizate este că organizația trebuie să furnizeze informațiile sau după caz, să dea curs solicitărilor în termen de cel mult o lună de la momentul transmiterii solicitării. În situații excepționale, termenul poate fi depășit însă numai în baza unei justificări temeinice.

Un aspect important de avut în vedere este faptul că organizației îi este permis să refuze solicitările persoanei vizate, dacă acestea sunt nejustificate sau excesive.

Pentru a răspunde cât mai rapid unor astfel de solicitări din partea persoanelor vizate, unele companii pun la dispoziția persoanelor vizate platforme online dedicate prin intermediul căreia pot fi verificate toate datele cu caracter personal prelucrate precum și toate elemente ce intră în componența dreptului de acces. După aceste verificări, persoana vizată poate opta să își exercite și alte drepturi prevăzute de GDPR – de exemplu, dreptul la rectificare sau dreptul de a fi uitat. O astfel de modalitate poate reprezenta o bună practică în ceea ce privește exercitarea drepturilor persoanelor vizate demonstrând nu numai responsabilitatea companiei, ci și transparența în relația cu persoana vizată.

Dreptul la rectificare¹⁷

Plecând de la definiția dată de GDPR acestei noțiuni („Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare”), este indicat ca organizația să se preocupe în prealabil de modalitățile în care se poate da eficiență acestui drept astfel încât, într-un timp scurt, să fie posibilă tratarea solicitării persoanei vizate.

De avut în vedere este faptul că acest drept nu este absolut și că pot fi identificate situații în care compania poate oferi un răspuns negativ persoanei vizate care își exercită acest drept. Mai mult decât atât, în funcție de specificul procesului de prelucrare, compania poate solicita dovezi care să susțină solicitarea persoanei vizate.

Dreptul la rectificare vizează, în practică, solicitări privind corectarea unor erori materiale legate de nume, număr de telefon, adresă de e-mail etc.

O platformă online dedicată exercitării unui astfel de drept poate permite persoanei vizate să identifice, într-o primă fază, toate elementele aferente dreptului de acces, urmând ca ulterior persoana vizată să aibă nu doar opțiunea exercitării dreptului la rectificare, ci și celelalte drepturi prevăzute de GDPR.

Dreptul de a fi uitat¹⁸

Dreptul la ștergerea datelor sau „dreptul de a fi uitat” („Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal, fără întârzieri nejustificate”) trebuie tratat de la caz la caz.

Nici acest drept nu trebuie privit ca un drept absolut, compania putând refuza, în situații justificate, exercitarea de către persoana vizată. De avut în vedere este însă faptul că responsabilitatea operatorului poate fi analizată inclusiv prin raportare la posibilitatea exercitării de către

¹⁷ Articolul 16 GDPR.

¹⁸ Articolul 17 GDPR.

persoanele vizate dată fiind importanța acestui drept ce asigură un nivel ridicat de protecție a datelor.

Ca bună practică, compania poate avea în vedere tratarea punctuală a ipotezelor în care persoanele vizate se pot adresa în vederea exercitării acestui drept, într-un limbaj accesibil.



● **Exemplu:** Mă pot adresa companiei pentru a-mi fi șterse datele?

Da, puteți solicita ștergerea datelor dumneavoastră, de exemplu atunci când datele personale nu mai sunt necesare.

Dreptul la restricționarea prelucrării¹⁹

Restricționarea intervine, de regulă, în cazurile în care nu este clar dacă și când vor trebui șterse datele cu caracter personal ale persoanei vizate.

Conform GDPR, acest drept poate fi exercitat atunci când este contestată exactitatea datelor în cauză, nu se dorește ștergerea datelor, datele nu mai sunt necesare în scopul pentru care au fost colectate, dar nu pot fi șterse încă din motive juridice sau după caz, când se așteaptă o decizie cu privire la obiecția persoanei vizate.

Ca bună practică, compania poate avea în vedere tratarea acestui drept prin oferirea unui răspuns și a unui exemplu concret în cadrul politicii privind exercitarea drepturilor, raportat la activitatea de prelucrare.



● **Exemplu:**

Întrebare: Ce presupune restricționarea prelucrării?

Răspuns: „Restricționarea” presupune faptul că prelucrarea datelor cu caracter personal se poate efectua numai cu consimțământul dumneavoastră pentru constatarea, exercitarea sau apărarea unui drept în justiție, pentru protecția drepturilor altei persoane fizice sau juridice sau din motive de interes public al UE sau al unui stat membru al UE. Veți fi informat(ă) înainte de ridicarea restricției.



● **Exemplu** (companie analizată: o unitate bancară ce oferă credite ipotecare): Dacă vă răzgândiți în ceea ce privește acordarea creditului

¹⁹ Articolul 18 GDPR.

și solicitați ștergerea tuturor datelor furnizate în vederea acordării creditului, având în vedere faptul că banca ar putea avea obligația să păstreze pentru o anumită durată de timp datele, vă puteți exercita dreptul la restricționare, pentru a vă asigura cu privire la faptul că datele dumneavoastră cu caracter personal nu vor fi prelucrate în scopuri pe care nu le doriți.

Dreptul la portabilitate²⁰

Portabilitatea datelor („Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal”) presupune returnarea datelor cu caracter personal furnizate sau transferul acestora către o altă companie, dacă acest lucru este posibil din punct de vedere tehnic.

Compania va informa persoana vizată cu privire la îndeplinirea condițiilor GDPR în ceea ce privește exercitarea acestui drept explicând, în același timp, faptul că, în cazul în care transferul de date cu caracter personal de la un mediu IT la altul nu este fezabil, persoana vizată va primi un răspuns negativ.

În ceea ce privește dreptul la portabilitatea datelor, compania ar trebui să se preocupe ca persoana vizată să înțeleagă:

- faptul că portabilitatea datelor presupune, în primul rând, un drept al persoanei vizate de a primi un subset de date cu caracter personal care o privesc și de a utiliza informațiile astfel obținute pentru uz personal ulterior;
- faptul că există facilitatea de a muta datele într-un alt mediu IT „fără obstacole”;
- faptul că persoana vizată are controlul asupra datelor pe care le obține exercitând acest drept;
- faptul că exercitarea dreptului la portabilitate nu presupune automat o ștergere a datelor după transferul datelor dacă persoana solicitată nu își exercită și dreptul la ștergerea datelor.

Suplimentar față de aspectele sus-menționate, în prezentarea acestui drept de către companie în cadrul politicii propuse, operatorul ar putea explica faptul că dreptul la portabilitate nu va opera pentru situațiile în care prelucrarea nu se bazează pe consimțământ sau contract.

²⁰ Articolul 20 GDPR.

Ca bună practică, se recomandă ca persoanele vizate să fie informate cu privire la condițiile în care operează portabilitatea datelor înainte să încheie orice cont pe care îl pot avea. Acest lucru permite persoanei vizate să țină cont de faptul că poate transmite cu ușurință datele către o altă companie sau către propriul dispozitiv înainte să opereze rezilierea contractului²¹.

Dreptul la opoziție²²

Dreptul la opoziție presupune ca organizația să pună la dispoziție un mecanism care să permită persoanei vizate să se opună prelucrării datelor sale personale, din motive legate de situația particulară în care aceasta se află sau atunci când datele sunt prelucrate în scopuri de marketing direct.

Comaniile vor avea în vedere obligația impusă de GDPR cu privire la acest drept, mai precis de a aduce în mod explicit în atenția persoanei vizate acest drept, cel târziu în momentul primei comunicări și de a-l prezenta în mod clar și separat de orice alte informații.

În informarea cu privire la dreptul de opoziție compania va avea în vedere identificarea situațiilor în care persoana vizată se poate opune pentru motive legate de propria persoană, respectiv:

- în cazul în care prelucrarea se bazează interesele legitime ale companiei sau ale unui terț;
- în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public;
- în cazul în care prelucrarea este realizată în scopuri de cercetare științifică sau istorică ori în scopuri statistice.

Dreptul de a nu face obiectul unei decizii automate²³

În cazul în care prelucrarea datelor se realizează prin mijloace tehnologice și nu presupune nicio implicare umană în procesul decizional, compania va informa persoana vizată cu privire la existența dreptului de a nu face obiectul unei decizii automate și cu privire la modalitățile și condițiile în care acesta operează. Concret, persoana vizată va fi informată

²¹ Ghid privind portabilitatea datelor (revizuit și adoptat în data de 5 aprilie 2017), Working Party 29.

²² Articolul 21 GDPR.

²³ Articolul 22 GDPR.

cu privire la faptul că are dreptul să își exprime opinia, să conteste decizia și să solicite ca decizia luată pe baza mecanismului automat să fie verificată prin intermediul factorului uman. La fel se va proceda și în cazul în care are loc o profilare, mai precis, atunci când se evaluează datele persoanei vizate pentru a se face anumite previziuni în legătura cu această persoană.

Compania ar trebui să ofere informații cu privire la efectele juridice sau la cele care pot afecta într-o măsură semnificativă persoana vizată, având în vedere specificul proceselor de prelucrare.

Deși, de regulă, persoana vizată nu poate face obiectul unei decizii bazate pe un mecanism automat de prelucrare, acest tip de proces decizional poate fi utilizat dacă legea permite utilizarea algoritmilor sau dacă există un consimțământ al persoanei vizate cu privire la acest tip de prelucrare.

Dreptul la retragerea consimțământului

Conform GDPR, retragerea consimțământului trebuie să se poată realiza cel puțin la fel de ușor ca acordarea acestuia.

Dacă prelucrarea de date are la bază consimțământul persoanei vizate, compania va informa persoana vizată cu privire la metodele în care poate opera retragerea consimțământului, luând în considerare modalitatea în care acesta a fost oferit, astfel încât să nu pună la dispoziția persoanei vizate un mecanism disproporționat prin raportare la metoda de colectare.

Dreptul de a formula o plângere la autoritatea de supraveghere

Politica privind exercitarea drepturilor persoanelor vizate tratează, în general, și dreptul persoanei vizate de a se adresa Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, în cazul în care consideră că drepturile prevăzute de GDPR nu au fost respectate.

Ca bună practică, compania poate avea în vedere să încurajeze persoana vizată să i se adreseze în vederea exercitării drepturilor și să se adreseze autorității numai după acest moment, în cazul în care nu se furnizează un răspuns în termen de o lună de la transmiterea solicitării sau după caz, dacă persoana vizată este nemulțumită de răspunsul primit. Anterior completării formularului de sesizare disponibil pe site-ul autorității, persoana vizată este întrebată dacă în prealabil s-a adresat companiei în

vederea soluționării problemei. Persoana vizată are două opțiuni de răspuns:

- DA, caz în care persoana vizată este informată cu privire la condițiile de admisibilitate a plângerii, putând ulterior fie să completeze formularul de plângere online, fie să descarce și să completeze formularul;

- NU, caz în care persoana vizată este informată cu privire la drepturile pe care le are și cu privire la faptul că în vederea exercitării drepturilor se va adresa companiei, în calitate de operator de date.

După ce persoana vizată își exercită dreptul sau după caz, drepturile în condițiile sus expuse, aceasta se poate adresa autorității cu plângere însoțită de dovezi, dacă operatorul nu a răspuns în termen sau dacă persoana vizată este nemulțumită de răspuns.

În ceea ce privește conținutul sesizării, persoana vizată va avea în vedere respectarea unor condiții privind identificarea, atât în ceea ce privește persoana sa, cât și în ceea ce privește compania dar și a unor condiții privind probele ce însoțesc plângerea.

În ceea ce privește identificarea, persoana vizată va furniza obligatoriu numele, prenumele, adresa de domiciliu sau de reședință, adresa pentru corespondență electronică²⁴. Nu este obligatoriu ca plângerea să fie depusă prin intermediul mijloacelor puse la dispoziție pe site-ul autorității, persoana vizată putând opta să transmită plângerea atât prin registratură cât și prin poștă. În lipsa elementelor de identificare, cererea va putea fi considerată ca fiind anonimă și poate fi clasată, fără ca autoritatea să transmită un răspuns.

De asemenea, se vor furniza toate datele deținute cu privire la companie, operator de date cu caracter personal sau imputernicit. Persoana vizată va identifica operatorul reclamat sau persoana imputernicită reclamată prin punerea la dispoziția autorității a numelui și prenumelui/denumirii, adresei/sediului sau cel puțin a informațiilor pe care le deține la momentul înaintării sesizării. În cazul în care plângerea este formulată prin reprezentant, în afara datelor persoanei vizate lezate se vor pune la dispoziția autorității și datele de contact ale reprezentantului: nume și prenume/denumire, adresă poștală de corespondență/sediu, adresă de corespondență electronică, număr de telefon și număr de înregistrare în registrul asociațiilor și fundațiilor, dacă este cazul.

Persoana vizată va preciza, pe lângă obiectul detaliat al plângerii, demersurile întreprinse la nivelul operatorului reclamat sau, după caz, al

²⁴ Adresa pentru corespondență electronică se va furniza obligatoriu doar în cazul în care plângerea este depusă online.

persoanei împuternicite reclamate. De asemenea, va anexa plângerii dovezi concludente în demonstrarea prejudiciului produs (de exemplu, solicitări, sesizări sau plângeri transmise în prealabil în vederea soluționării problemei ce face obiectul sesizării, eventualele răspunsuri primite etc.). În plus, în cazul plângerilor având ca obiect dreptul la viața intimă, familială și privată în domeniul comunicațiilor electronice/comerțului electronic, inclusiv prin transmiterea de comunicări nesolicitate, persoana vizată va pune la dispoziția autorității de supraveghere mesajele primite în formatul original, capturi de pe telefon din care să rezulte fie sms-ul primit fără o solicitare prealabilă sau, după caz, numărul de telefon de la care persoana vizată a fost contactată etc.

Dreptul de a se adresa instanțelor de judecată

Unul dintre drepturile cu privire la care compania ar trebui să informeze operatorul de date este dreptul persoanei vizate care a suferit un prejudiciu material sau moral urmare a încălcării prevederilor legale privind protecția datelor de către companie să se adreseze instanței competente în vederea obținerii de despăgubiri.

Există companii care au optat să pună la dispoziția persoanelor vizate platforme dedicate în vederea exercitării drepturilor prevăzute de GDPR, integrând în politica privind exercitarea drepturilor un instrument practic prin intermediul căruia persoana vizată poate dispune direct de toate aceste drepturi, în limitele legale.

Acest demers constituie o bună practică, avantajul principal oferit de compania care optează pentru o astfel de platformă constând în faptul că persoana vizată nu este îndrumată să depună o solicitare prin intermediul corespondenței electronice sau prin poștă ori registratură, ci poate accesa de îndată categoriile de date prelucrate, putând dispune de orice drept cu privire la acestea, scutindu-se, în acest mod, o serie de proceduri interne aferente de tipul: S-a primit solicitarea, unde ajunge? Cine răspunde? Care este deadline-ul pentru răspuns? și cel mai important lucru al zilelor noastre, timpul.

Politica privind retenția datelor

Un astfel de document tratează, de regulă, atât partea de actualizare a datelor, cât și duratele propriu-zise pe care operatorul le are în vedere pentru stocarea datelor, plecând de la obligațiile impuse de prevederile

legale aplicabile. Desigur, companiile pot opta pentru o procedură distinctă pentru actualizarea datelor cu caracter personal, document ce va descrie pașii urmați intern pentru verificările privind duratele stocării datelor, actualizarea acestora și dacă este cazul, pentru ștergerea datelor pentru care se constată că a expirat durata de retenție stabilită la nivel de companie.

În vederea redactării Politicii privind retenția datelor, compania se va raporta, în principal, la prevederile legale în vigoare privind păstrarea documentelor ce ar putea conține date personale, urmărindu-se specificul activității desfășurate de operator. Spre exemplu, compania va ține cont de termenele instituite de Legea Arhivelor Naționale²⁵ privind păstrarea documentelor medicale – 100 de ani de la crearea lor sau pentru dosarele personale – 75 de ani de la crearea lor. De asemenea, compania va lua în considerare termenele instituite prin intermediul Ordinului Ministerului Finanțelor Publice nr. 2634/2015 pentru păstrarea documentelor contabile – state de salarii – 50 de ani, registre – 10 ani, chitanțe, dispoziții de plată, ordin de deplasare, decont de cheltuieli, decizie de imputare, angajament de plată – 5 ani, începând cu data încheierii exercițiului financiar în cursul căruia au fost întocmite. Nu în ultimul rând, compania se va raporta la termenul de 30 de zile pentru păstrarea datelor colectate în cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video la locul de muncă, stabilit de Legea privind măsurile de aplicare GDPR²⁶.

Sigur că legislația nu este acoperitoare în ceea ce privește stabilirea duratelor de retenție, motiv pentru care operatorul va institui, pentru anumite categorii de documente ce conțin date cu caracter personal, perioade de retenție proporționale cu scopul prelucrării de date. Ca o regulă generală, compania se poate raporta, acolo unde legea un prevede o perioadă precisă pentru retenție, la termenul general de prescripție de 3 ani calculat de la momentul încetării prelucrării. Cu toate acestea, compania va avea în vedere faptul că această durată ar putea fi una excesivă, prin raportare la scop și va decide în sensul limitării stocării, instituind o durată de retenție redusă.

²⁵ Legea nr. 16/1996 a Arhivelor Naționale.

²⁶ Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

! **Exemplu** (date păstrate cu termene stabilite de companie): În vederea recrutării de personal, compania colectează CV-uri ale candidaților. Neexistând un termen impus prin intermediul unui act normativ cu privire la stocarea acestui tip de document, la nivel intern se va stabili o durată de retenție proporțională cu scopul. De regulă, companiile optează să elimine CV-urile avute în vedere pentru un proces de recrutare după finalizarea perioadei de recrutare însă pot exista și situații în care operatorul decide să păstreze CV-urile pentru o durată mai lungă de timp astfel încât să se poată folosi de informațiile colectate și în cadrul viitoarelor procese de recrutare.

Provocarea oricărei companii în materie de retenție a datelor apare acolo unde legea nu stabilește termene de stocare precise, iar managementul companiei trebuie să stabilească, prin raportare la scop, duratele de retenție potrivite pentru anumite categorii de date. În practică se conturează o serie de categorii de date pentru care nu se cunoaște durata de retenție „potrivită”, cum ar fi datele din CV-uri, recomandări ale foștilor angajatori, scrisori de intenție, date colectate prin intermediul platformelor online, date colectate în vederea derulării de campanii și concursuri, date colectate prin intermediul registrelor de pază, date colectate prin intermediul sistemelor de supraveghere GPS etc.

Responsabilitatea companiei în materie de retenție a datelor nu se oprește însă aici. Mai departe, compania va trebui să se preocupe să respecte perioadele de retenție pe care le stabilește și va distruge documentele pentru care a expirat durata de retenție. Sigur că distrugerea documentelor pentru care a expirat durata de retenție vizează un doar partea fizică – documentele tipărite, ci și documentele în format electronic.

Politica de retenție ar trebui însă văzută ca un mare avantaj pentru companiile care se confruntă cu un volum foarte mare de documente. Durata de retenție poate fi un instrument eficient în eliberarea birourilor și a arhivelor în care, după cum bine știm, se păstrează foarte multe documente – unele chiar inutile, plecând de la principiul „nu se știe când avem nevoie de ele”.

Un alt aspect pe care ar trebui să îl prevadă o politică de retenție vizează metodele de distrugere a documentelor pentru care a expirat durata de stocare, în special în ceea ce privește documentele pe suport hârtie. Astfel de documente nu ar trebui aruncate la gunoi, fiind deja cunoscute cazuri în care asemenea practici au condus la breșe de securitate. Pentru a se asigura de faptul că documentele sunt distruse

Într-o manieră care să nu permită identificarea datelor personale ori a informațiilor confidențiale în general, companiile apelează, de regulă, la utilizare unui shredder. Desigur, în funcție de opțiunile disponibile, se poate opta și pentru contractarea unei societăți care să ducă la îndeplinirea sarcina de distrugere a documentelor pentru care a expirat durata de retenție, caz în care compania va avea în vedere să își ia toate precauțiile necesare, astfel încât rezultatul să nu compromită acest proces sensibil. În ceea ce privește documentele în format electronic, se poate opta nu doar pentru distrugere, ci și pentru anonimizare sau pseudonimizare.

Procedura pentru incidente de securitate

Majoritatea companiilor sunt în temă cu privire la faptul că o breșă de securitate impune informarea autorității de supraveghere, această informație fiind amplu dezbătută în contextul aplicării GDPR.

Analizând politicile interne ale companiilor, putem observa faptul că s-a optat fie pentru suprapunerea noțiunilor de „incident de securitate” și „breșă de securitate”, fie pentru departajarea acestora, incidentul de securitate având, de regulă, o gravitate mai mică prin raportare la breșa de securitate.

Într-o prima fază, se consideră că orice acțiune care duce la distrugerea, pierderea, modificarea sau divulgarea ori accesarea neautorizată a datelor cu caracter personal aparținând unei companii intră în sfera incidentelor de securitate.

Concret, dacă ar fi să ne imaginăm situațiile care pot conduce la încadrarea acestora în incidente de securitate, vom realiza faptul că în cadrul activităților pe care le desfășurăm le întâlnim frecvent. Pierderea unui telefon ce nu avea setat un cod de acces și pe care sunt stocate numere de telefon și este permis accesul la e-mailul companiei, transmiterea unui e-mail către o altă persoană decât destinatarul, pierderea sau furtul unui laptop al companiei – toate acestea intră în sfera incidentelor de securitate. Iar exemplele pot continua, în funcție de specificul activității operatorului și de complexitatea proceselor de prelucrare. Așadar, companiile trebuie să înțeleagă, într-o primă fază, faptul că nu doar furtul de baze de date sau hacking-ul/cracking-ul reprezintă incidente de securitate.

După exemplificarea situațiilor ce s-ar putea încadra în sfera incidentelor de securitate, politica ar trebui să descrie pașii de urmat pornind de la analiza internă efectuată de către management și DPO.

Ancheta internă efectuată la nivel de management ar trebui să identifice următoarele aspecte:

- categoriile și numărul aproximativ de persoane vizate implicate;
- categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- natura încălcării datelor cu caracter personal;
- consecințele probabile ale încălcării datelor cu caracter personal;
- dacă este cazul, măsurile urgente ce pot fi implementate în vederea diminuării consecințelor apărute în urma incidentului.

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal trebuie notificată cu privire la breșa de securitate în termen de 72 de ore de la confirmarea încălcării de către managementul companiei, chiar dacă toate informațiile nu sunt încă disponibile. Notificarea se realizează utilizând formularul tipizat disponibil pe site-ul www.dataprotection.ro și cuprinde următoarele elemente: identificarea operatorului, informații inițiale, informații suplimentare, eventuale informări suplimentare și eventuale aspecte transfrontaliere.

Secțiunea 1

Notificarea operatorului

1. Denumirea operatorului: Ajutor

Sector privat ☐ Sector public ☐

Numere/Denumirea operatorului:

CFRUA:

2. Identitatea și datele de contact ale responsabilului cu protecția datelor sau ale unui alt punct de contact de unde se pot obține mai multe informații: Ajutor

Nume și prenume responsabilului:

Adresă/Sediu:

Telefon: E-mail:

3. Este notificarea nouă sau o completare a notificării inițiale?

Notificare nouă ☐ Completare notificare nr. se va breca numărul de înregistrare al notificării din registrul general al autorității

Trimite formularul

Câmpurile marcate cu * sunt obligatorii

Informații inițiale privind încălcarea securității datelor cu caracter personal (se vor specifica în completările ulterioare, dacă este cazul)

4. Data și ora incidentului (dacă se cunosc; dacă este necesar, se poate face o estimare) și ale depășirii incidentului

4.1 Data și ora incidentului: 13/05/2020 12:40 (oo mm) 4.2 Data și ora depășirii incidentului: 13/05/2020 12:40 (oo mm)

5. Caracterul încălcării securității datelor cu caracter personal (de exemplu: confidențialitate/integritate/disponibilitate)

6. Natura și conținutul datelor cu caracter personal în cauză

7. Măsurile tehnice și organizatorice aplicate (sau care urmează a fi aplicate) de către operator

8. Utilizarea relevanței altor operatori (dacă este cazul)

Trimite formularul

Câmpurile marcate cu * sunt obligatorii

I. Informații suplimentare privind încălcarea securității datelor cu caracter personal

9. Rezumatul incidentului care a generat încălcarea securității datelor cu caracter personal (inclusiv localizarea fizică a încălcării și suporturile de stocare implicate)

10. Numărul persoanelor fizice vizate (estimare, după caz)

11. Evenimentele consecințe și efecte adverse (riscuri) pentru persoanele fizice vizate

12. Măsurile tehnice și organizatorice luate de operator în scopul atenuării eventualelor efecte negative

Câmpurile marcate cu * sunt obligatorii.

Trimite formularul

II. Evenuale informații suplimentare către persoanele fizice vizate

13. Conținutul informațiilor sau motivele pentru care nu s-a făcut informarea persoanelor fizice vizate

14. Mijloace de comunicare utilizate pentru transmiterea informațiilor

15. Numărul persoanelor fizice vizate informate

Câmpurile marcate cu * sunt obligatorii.

Trimite formularul

III. Evenuale aspecte transfrontaliere

16. Încălcarea a securității datelor cu caracter personal care implică persoane fizice vizate din alte state membre

Da ☐ Nu ☐

17. Notificarea altor autorități naționale competente

Da ☐ Nu ☐

Dacă da, menționați autoritățile competente:

Câmpurile marcate cu * sunt obligatorii.

Trimite formularul

La nivelul companiilor ce activează în domeniul comunicațiilor electronice, politica va fi redactată într-o manieră care să permită parcurgerea mai rapidă a anchetei interne, termenul pentru notificare fiind, pentru această categorie de operatori, de 24 de ore.

Notificarea încălcării securității datelor pentru acest segment se realizează prin intermediul unui formulat distinct, disponibil pe site-ul www.dataprotection.ro, ce cuprinde aceleași elemente esențiale.

- Puteam avea politica suport hârtie;
- Politica email;
- Politica imprimare;
- Politica utilizare stick;
- Politica călătorie bagaj;
- Politica interdicție dezinstalare antivirus malware;
- Clean desk.

Evaluarea partenerilor comerciali

Ca o bună practică, anterior semnării unui contract de parteneriat, în special, dacă obiectul acestuia impune procese de prelucrare de date în comun sau în numele companiei, se poate avea în vedere evaluarea partenerului.

Evaluarea se realizează, de regulă, prin intermediul unui chestionar/checklist pentru verificarea preliminară a practicilor de securitate și confidențialitate.

Această măsură demonstrează diligența companiei în ceea ce privește alegerea partenerilor contractuali. În funcție de răspunsurile oferite sau după caz, de refuz, compania poate concluziona asupra garanțiilor pe care le oferă cealaltă parte. Sigur că la momentul verificărilor prealabile este posibil ca partenerul să nu îndeplinească toate criteriile privind securitatea și confidențialitatea pe care le urmărește compania, însă în cadrul negocierilor precontractuale se poate accepta un angajament conform căruia până la momentul semnării contractului toate eventualele deficiențe se vor remedia.

Aspectele supuse verificării ar putea include existența unor politici și proceduri interne privind securitatea și confidențialitatea, măsurile tehnice și organizatorice implementate (eventual se poate solicita o scurtă descriere a acestor măsuri), desemnarea unui DPO intern sau extern, accesul limitat la date, instruirea salariaților care primesc acces la date, existența unor acorduri de confidențialitate cu privire la date, capacitatea de a ține o evidență a operațiunilor de prelucrare rezultate din executarea contractului, gestionarea incidentelor de securitate, disponibilitatea în a pune la dispoziția companiei politicile și procedurile de lucru, informații și echipamente cu privire la prelucrările de date rezultate din executarea contractului etc. În funcție de specificul obiectului contractului, evaluarea poate intra în detalii precum existența unor testări de securitate/auditi IT, certificări precum ISO 27001, existența unor plângeri la A.N.S.P.D.C.P. în ultimii ani, ultima actualizare a politicilor și procedurilor privind protecția datelor cu caracter personal etc.

Note de informare

Această măsură este foarte întâlnită în practică, necesitatea acestui document rezultând din obligația de informare a persoanelor vizate. Fie că ne raportăm la angajați, fie că avem în vedere parteneri comerciali sau

vizitatori ai unei arii în care există un sistem video sau de termometrizare ori ai unui site, identificăm aceste note de informare fie denumite prin raportare la termenul „informare”, fie politici ori proceduri. În orice caz, important de avut în vedere este faptul că nu prezintă relevanță denumirea documentului ce asigură informarea, ci conținutul acestuia, care trebuie să demonstreze îndeplinirea obligației de informare.

Conținutul notelor de informare diferă în funcție de două criterii, după cum urmează: dacă datele colectate sunt furnizate de persoane vizate și dacă datele sunt obținute. În cazul în care datele cu caracter personal sunt obținute și nu furnizate direct de către persoana vizată, compania are o serie de obligații suplimentare cu privire la informare, incluzând, dar nelimitându-se la: precizarea duratei de retenție, existența drepturilor cu privire la date inclusiv cu privire la retragerea consimțământului, existența unui proces decizional automat etc. Cu toate acestea, majoritatea companiilor optează pentru o informare cât mai completă a persoanelor vizate, astfel încât furnizează aceste elemente chiar și atunci când datele sunt colectate direct de la persoana vizată.

Informarea salariaților și a aplicanților pentru un post disponibil în cadrul companiei

O notă de informare a salariaților cu privire la datele prelucrate de către angajator în cadrul relațiilor de muncă ar putea cuprinde, pe lângă datele angajatorului și dacă este cazul, ale DPO-ului desemnat, scopurile în care sunt prelucrate datele (EXEMPLU: eliberarea de adeverințe de salariat sau de documente din dosarul de salariat, pentru realizarea activității de instruire periodică în domeniul securității și sănătății în muncă, pentru realizarea examinării medicale la angajare sau periodică, pentru cercetarea, identificarea cauzelor ce au condus la apariția accidentelor de munca și comunicarea acestora către Inspectoratul Teritorial de Munca, pentru instruirea periodică în domeniul protecției datelor cu caracter personal, pentru depunerea declarațiilor în sisteme de pensii, șomaj, sănătate, pentru organizarea de evenimente interne, în vederea asigurării pazei și securității angajaților și a bunurilor societății etc.), categoriile de date prelucrate în aceste scopuri, măsuri implementate, perioadă de retenție, transfer internațional etc.

Informarea candidaților ar putea include informații privind păstrarea datelor din CV după finalizarea procesului de recrutare, durata de retenție, drepturile pe care persoana vizată le are cu privire la datele prelucrate etc.

În cazul unor obligații legale temporare, așa cum a fost cazul preluării de date prin intermediul termometrării pe durata pandemiei provocată de apariția virusului SARS-CoV-2, atât salariații cât și candidații puteau fi informați prin afișarea unor note de informare în punctele de colectare a temperaturii.

De asemenea, în ceea ce privește sistemele de monitorizare video și/sau GPS, angajatorul poate opta, pe lângă o notă informativă, să afișeze pictograme și/sau după caz, stickere specifice în interiorul autovehiculelor monitorizate.

Informarea partenerilor/clientilor

Aspectele privind informarea partenerilor ori a clienților în general se regăsesc inserate, de cele mai multe ori, în contracte. Separat de angajamentele pe care părțile și le asumă cu privire la procesele de prelucrare derivate din executarea contractului, părțile se pot informa reciproc cu privire la categoriile de date puse la dispoziție, măsurile tehnice și organizatorice implementate, garanții oferite etc.

În ceea ce privește informarea clienților, companiile pot opta pentru transmiterea unor note de informare ori afișarea lor pe un panou ori pe o tabletă. În orice caz, preocuparea principală trebuie să fie ca persoana vizată să aibă acces cât mai ușor la informațiile privind prelucrarea de date cu caracter personal.

Informarea vizitatorilor

Implementarea unor sisteme de monitorizare video sau a temperaturii (de exemplu, prin intermediul unei porți de verificare a temperaturii corporale – măsură destul de răspândită la nivelul spațiilor comerciale pe durata pandemiei din anul 2020) ori a unor mijloace prin intermediul cărora se colectează MAC-ul dispozitivului prin conectarea automată la rețeaua de internet, impune informarea persoanelor vizate ale căror date cu caracter personal pot fi colectate prin intermediul acestei metode.

De regulă, notele de informare aferente acestor procese de prelucrare prevăd elementele de bază impuse de obligația de informare ce este în sarcina operatorului conform GDPR și sunt afișate fie în format fizic, uneori însoțite de pictograme specifice sau, după caz, în format electronic, pe tablete sau alte echipamente similare ori după caz, pe dispozitivul propriu utilizat pentru conectarea la internet.

Ca bună practică, compania poate avea în vedere, în ceea ce privește procesele de prelucrare rezultate din conectarea automată a unui dispozitiv la rețele de tipul Free WiFi, să transmită o notă de informare completă asupra datelor pe dispozitivul personal ce utilizează rețeaua respectivă. Având în vedere faptul că prelucrarea se realizează în interes legitim, iar dispozitivul are aptitudinea de a se conecta automat la o rețea de internet, fără o acțiune propriu-zisă din partea persoanei vizate, afișarea notelor de informare ar putea fi ineficientă deoarece persoana vizată, în momentul în care se află în interiorul unui spațiu comercial ori chiar și în apropierea acestuia, nu se poate aștepta în mod rezonabil ca anumite date cu caracter personal să fie prelucrate pentru analiza comportamentului său (când a intrat în aria rețelei de internet, cât timp a petrecut într-o anumită locație etc.). Pentru astfel de practici recomandăm totuși obținerea unui consimțământ din partea persoanelor vizate, deoarece o analiză a interesului legitim cu greu ar putea concluziona asupra faptului că interesele legitime ale operatorului prevalează dreptului la intimitate și la viață privată al persoanei vizate.

Consultarea reprezentanților angajaților cu privire la sisteme ce presupun prelucrări de date în spațiile în care se desfășoară activitate

Instrumentul consultării angajaților este obligatoriu atunci când operatorul intenționează să implementeze mijloace de supraveghere video în sediile sau în punctele de lucru în care salariații desfășoară activitate. Ca bună practică, angajatorul poate apela însă la această măsură pentru mai multe procese de prelucrare, precum utilizarea de mijloace GPS, utilizarea de mijloace de verificare a stațiilor de lucru și în general cu privire la orice proces de prelucrare susceptibil să aducă atingere dreptului la viață privată a salariatului.

În prezent, angajatorii pun accent pe uniformitate, eficiență, productivitate și nu, în ultimul rând, pe control și pentru atingerea acestor obiective este clar că se dorește utilizarea de noi tehnologii ce prezintă însă dezavantajul de a fi susceptibile a aduce atingere vieții private a angajaților. Date fiind riscurile asociate prelucrării datelor angajaților prin intermediul mijloacelor de prelucrare ce prezintă acest factor de risc, angajatorii trebuie să aibă în vedere, pentru asigurarea legalității procesului de prelucrare, transparența în raport cu salariații organizației, minimizarea datelor prelucrate și nu în ultimul rând, proporționalitatea mijloacelor folosite în cadrul proceselor de prelucrare.

Înainte de a utiliza un sistem de geolocalizare ori de verificare a stațiilor de lucru, angajatorul ar putea consulta reprezentanții salariaților pentru a spori garanțiile oferite și pentru a demonstra diligență în raport cu aceste prelucrări „speciale”. Ulterior, angajatorul va stabili scopul în care colectează datele, în conformitate cu cerințele GDPR. Mai departe, pentru a putea demonstra respectarea GDPR, se recomandă, ca bună practică, ca angajatorul să transpună în scris și pentru fiecare sistem/categorie de mijloace în parte, scopul determinat al prelucrării. În ceea ce privește acest scop determinat, European Data Protection Board avertizează asupra faptului că supravegherea video bazată pe simplul scop al siguranței nu este suficient de specific²⁷. De asemenea, dispozitivele de urmărire a vehiculelor nu ar trebui să aibă drept scop urmărirea sau monitorizarea comportamentului sau a locației în care se află conducătorii auto²⁸. Din aceste motive, compania va proceda la stabilirea și explicarea, prin raportare la situațiile de fapt cu care s-a confruntat, a necesității mijloacelor pe care dorește să le implementeze. Suportul DPO-ului se poate dovedi extrem de important în astfel de decizii pe care managementul dorește să le implementeze. Sigur că avizul DPO-ului poate fi și unul negativ, managementul urmând să decidă dacă ține cont de recomandările responsabilului sau dacă își asumă riscurile aferente unei prelucrări de date nelegale.

Provocările pot apărea atunci când angajatorul dorește să instaleze mijloace biometrice pe bază de tehnologii cu recunoaștere facială. Deși în mod normal un angajator ar trebui să se abțină de la utilizarea unor astfel de sisteme, pe bază de justificare temeinică, suntem de părere ca astfel de mijloace pot fi utilizate. Angajatorii ar putea fi tentați să se orienteze spre obținerea unui consimțământ de la angajați, însă având în vedere dezechilibrul de puteri existent într-un raport de muncă, dat de relația de subordonare, se consideră că angajații nu sunt aproape niciodată în măsură să își exprime, să refuze sau să își revoce în mod liber consimțământul²⁹. Așadar, și cu privire la aceste sisteme, este bine să se recurgă la consultarea reprezentanților salariaților astfel încât decizia finală să nu fie una impusă unilateral de angajator, ci rezultată în urma unor „negocieri” cu salariații. Și în cadrul acestui demers există riscul ca reprezentantul să nu fie de acord, în numele întregului colectiv cu noile

²⁷ EDPB. Ghidul nr. 3/2019 privind prelucrarea datelor personale prin intermediul mijloacelor video – v.2.0.

²⁸ WP 29. Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă, versiunea în limba română.

²⁹ WP 29. Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă.

mijloace pe care angajatorul intenționează să le implementeze, însă în funcție de argumentele prezentate în cadrul consultărilor, managementul companiei poate opta pentru utilizarea sistemelor, nefiind ținut finalmente în deciziile sale nici de salariați și nici de DPO.

În urma consultării reprezentantului angajaților, se recomandă încheierea unui proces-verbal din care să rezulte planul angajatorului, situațiile de fapt anterioare de avut în vedere pentru circumstanțiere, opiniile reprezentantului și decizia finală la care acesta a ajuns în urma discuțiilor purtate cu managementul companiei și cu DPO-ul.

Acordurile privind protecția datelor cu caracter personal

Acordurile ce stabilesc obligațiile și garanțiile pe care părțile le au în vedere cu privire la procesele de prelucrări de date pot fi semnate în cadrul negocierilor precontractuale sau ulterior acestui moment, ori pot fi incluse într-o secțiune dedicată chiar în conținutul contractului. Fie că ne referim la operatori asociați, la împuterniciți ori chiar la proprii salariați ca subiecți ai unor astfel de clauze specifice, compania va avea în vedere faptul că forma acestui acord nu este una standard.

În practică, aceste acorduri sunt identificate sub denumirea de DPA – Data Protection Agreement și se confundă adesea cu bine cunoscutele NDA-uri (Non Disclosure Agreement) pe care companiile le încheie pentru a-și proteja informațiile confidențiale în cadrul unor negocieri ori pe durata executării unui contract ce presupune un schimb de informații sensibile. Sigur că orice clauză cuprinsă într-un DPA se poate regăsi și într-un NDA, fiind chiar recomandat ca un NDA să nu se limiteze la protejarea unor informații legate de dezvoltarea propriu-zisă a relației contractuale principale (secrete comerciale, idei, know-how, șabloane, manuale, rapoarte etc.) și să se extindă în direcția datelor cu caracter personal, tratându-le ca date confidențiale.

Dacă ne raportăm la acordurile operator – împuternicit, se va avea în vedere faptul că un astfel de instrument trebuie avut în vedere doar după o verificare prealabilă a garanțiilor oferite de cealaltă parte. În măsura în care compania, în calitatea sa de operator de date, a efectuat această verificare din care a rezultat faptul că împuternicitul oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate astfel încât prelucrarea să respecte cerințele legale în general și pe cele ale operatorului în mod particular, se poate încheia acordul de prelucrare, cu respectarea condițiilor prevăzute de Regulament. Într-o

astfel de ipoteză, evaluarea partenerilor comerciali descrisă într-o secțiune anterioară își poate dovedi eficiența, jucând un rol important în găsirea partenerului comercial „ideal”. Sigur că există și ipoteza în care compania poate întâmpina scenariul în care partenerul nu a implementat cerințele legale în materie de protecție a datelor, aspect ce poate constitui un risc pentru companie, mai ales în contextul în care cealaltă parte ar trebui să între, prin prisma contractului ce se dorește a fi încheiat, în posesia unui volum de date foarte importante pentru operator. Într-o astfel de situație, se recomandă ca operatorul să obțină de la partenerul comercial un angajament în baza căruia vor fi implementate măsuri tehnice și organizatorice adecvate care să permită executarea contractului cu protejarea datelor ce vor face obiectul transferurilor între părți.

Exemplu: O companie dorește să externalizeze activitatea departamentului de resurse umane. În acest sens, încep negocierile în vederea identificării unui furnizor care să satisfacă cerințele companiei în materie de resurse umane. Căutările efectuate au identificat partenerul care ar putea satisface exigențele companiei în materie de resurse umane, însă în urma completării chestionarului pentru evaluarea partenerilor comerciali, a rezultat faptul că potențialul furnizor nu implementează planuri și politici privind confidențialitatea și securitatea datelor cu caracter personal, că accesul la date nu este restricționat strict pentru salariații care ar fi implicați în colaborare, că nu a fost desemnat un DPO, că nu are capacitatea de a păstra un registru al prelucrărilor de date ce ar rezulta din executarea contractului etc. Cu toate acestea, compania poate decide să îi ofere furnizorului un termen în care să se conformeze acestor cerințe, astfel încât contractul principal să se poată derula în condiții de siguranță pentru ambele părți.

Cu titlu de exemplu, calitatea de împuternicit poate fi avută în vedere pentru furnizorii de servicii de resurse umane/pay-roll, așa cum am arătat mai sus, de IT, contabilitate, sănătatea și securitate în muncă, marketing etc.

Chestionarul pentru evaluarea partenerului comercial necesar pentru efectuarea analizei descrisă într-o secțiune anterioară poate fi particularizat astfel încât să devină un chestionar de evaluare a persoanelor împuternicite prin intermediul căruia compania se poate lămurii cu privire la nivelul de conformare al potențialului furnizor văzut ca împuternicit.

Acordurile de prelucrare între operatorii asociați ar trebui să aibă în vedere, cu titlu prealabil, o verificare a partenerului, astfel încât operatorul să se asigure cu privire la oferirea garanțiilor adecvate. Având în vedere faptul că operatorii asociați stabilesc în comun scopurile și mijloacele de

prelucrare, DPA-ul va reprezenta instrumentul prin intermediul căruia sunt stabilite în mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea cerințelor Regulamentului.

Pe lângă obiectul și durata prelucrării, natura prelucrării, categoriile de date și de persoane vizate, acordul de prelucrare conține instrucțiunile clare ale operatorului ce stabilesc anumite limite în ceea ce privește relația cu împuternicitul, interdicția împuternicitului de a încheia un contract cu un subîmputernicit fără acordul operatorului exprimat în prealabil, obligația de a asista operatorul în ceea ce privește securitatea prelucrării, notificarea încălcării securității datelor, în elaborarea evaluărilor de impact, în păstrarea registrului de prelucrări etc.

În practică pot fi identificate multe dificultăți în vederea încheierii acordurilor, deoarece operatorii sunt obligați să își distribuie responsabilitatea pe o lista foarte lungă de elemente. Practic, operatorii se vor pune de acord cu privire la elemente precum scopul în care sunt prelucrate datele cu caracter personal, temeiul juridic al prelucrării, perioada pentru care fiecare operator va păstra datele sau, dacă acest lucru nu este posibil, criteriile avute în vedere pentru a determina durata de retenție, interesele legitime și, nu în ultimul rând, aspecte privind eventualele transferuri internaționale. În funcție de riscurile identificate de fiecare operator asociat, acesta poate solicita introducerea în acord a unor criterii care să asigure protejarea datelor ce fac obiectul prelucrării stabilite în comun de cei doi operatori.

O problemă pe care o identificăm foarte des constă în faptul că părțile unui acord nu cunosc foarte clar încadrarea pe care trebuie să o aibă în vedere prin raportare la specificul relației contractuale principale. De multe ori, identificăm operatori încadrați ca împuterniciți, uneori chiar și în ipotezele în care nu se intră în contact cu alte date cu caracter personal în afara celor generale, existente într-un contract precum nume și prenume ale reprezentanților, funcție și semnătură – discutăm în această ipoteză despre acei operatori care își încadrează automat orice colaborator în noțiunea de împuternicit ori operatori care se raportează la un împuternicit când în realitate raportul dintre părți descrie o relație juridică de tipul operator – operator.

Nu ar trebui exclusă din discuție ideea conform căreia putem întâlni acorduri între operatori, fără ca aceștia să fie asociați, fiecare fiind în mod independent răspunzător de prelucrările de date efectuate.



● **Exemplu:** O companie se află în negocieri cu o altă companie care deține mai multe săli de fitness. Compania dorește deschiderea unei

săli de fitness la care să primească acces doar angajații săi, în incinta locației se desfășoară activitatea. Sala de fitness va funcționa însă în baza propriilor reguli, fiecare angajat semnând un contract cu furnizorul de servicii de fitness, prezumându-se ca orice persoană care intră în incinta sălii de fitness și solicită un pachet de servicii este salariatul companiei. Cu alte cuvinte, sala funcționează individual, neoferind companiei informații cu privire la numele beneficiarilor serviciilor ori alte date cu caracter personal. Compania încheie practic un contract în baza căruia pune la dispoziție un spațiu și eventual plătește o anumită sumă de bani conform convenției părților, fără a intra în posesia datelor cu caracter personal ale salariaților ce beneficiază de aceste servicii. Analizând acest raport juridic, este clar că este exclus să privim relația ca fiind una de tipul operator – împuterniciți sau între operatori asociați.

Auditul intern

Acest instrument de verificare apare ca fiind absolut necesar la demararea procesului de conformare. Ulterior, ca bună practică, este recomandat să se reia procesul de auditare, cel puțin o dată pe an. Nu în ultimul rând, trebuie precizat faptul că orice proces de prelucrare privit separat poate fi supus auditării în orice moment, fiind chiar recomandat ca în special în cazul noilor procese de prelucrare să se parcurgă un audit care să identifice eventualele vulnerabilități și măsuri de implementat pentru diminuarea sau după caz, eliminarea riscurilor asociate prelucrării analizate.

Auditul preliminar

Auditul pe care compania îl realizează la începutul procesului de conformare are ca obiectiv colectarea tuturor informațiilor privind nivelul actual al conformității, identificarea riscurilor prin raportare la cerințele Regulamentului și ale legislației naționale și în final, identificarea măsurilor ce urmează să fie implementate etapizat pentru a se ajunge, treptat, la obiectivul dorit de companie, anume asigurarea unui nivel optim de conformitate prin prioritizarea diminuării/eliminării riscurilor derivate din acțiunile privind prelucrări de date cu caracter personal.

Pentru a fi atins însă acest obiectiv, este foarte important ca managementul companiei să se implice și să identifice angajații și/sau colaboratorii care pot ajuta la stabilirea stării de fapt a proceselor de prelucrări de date.

Auditul este demarat numai după stabilirea metodologiei ce va fi folosită în vederea efectuării verificărilor. Se poate urma un sistem bazat pe Q&A, urmând ca, pe baza răspunsurilor oferite de companie, să se realizeze raportul de audit, însă se recomandă să existe mai multe întâlniri pentru a discuta asupra detaliilor privind procesele de prelucrare cu persoanele responsabile din interiorul companiei, de exemplu coordonatorul Departamentului Resurse Umane, Financiar-Contabilitate, Vânzări, Securitate etc., astfel încât informația ce se regăsește în raport să fie bazată pe relatarea fidelă a situației de fapt existente. Nu în ultimul rând, un audit eficient presupune și analiza documentelor utilizate intern la nivelul diferitelor departamente dar și participarea directă a persoanelor care efectuează auditul la procesele societății, pentru a observa, spre exemplu, procesele din fabrică, din arhivă, funcționarea efectivă a activității de call-center etc.

Auditul preliminar poate fi avut în vedere și dacă se dorește o altă abordare asupra procesului anterior de implementare a cerințelor GDPR. Multe companii se regăsesc în situația în care consideră că măsurile implementate nu sunt suficiente în a asigura conformitatea. În astfel de situații, se recomandă parcurgerea unui nou audit preliminar care să stabilească nivelul de conformitate ulterior implementării măsurilor implementate în urma auditului anterior.

Raportul de audit

Raportul de audit este documentul ce se întocmește la finalul auditului, fie preliminar, fie temporar. În urma procesului de auditare, va rezulta Planul de conformare. Compania va avea în vedere faptul că acest plan de conformare trebuie privit ca fiind într-o dinamică continuă, dat fiind ritmul accelerat în care se modifică aspectele organizaționale interne.

Raportul de audit va identifica în concret procesele de prelucrare interne analizate. Se poate avea în vedere o abordare pe mai multe segmente, în funcție de activitățile principale ale operatorului sau după caz, în funcție de departamentele identificate în organigrama pusă la dispoziție de către companie.

Într-o primă etapă se recomandă să se stabilească scopurile avute în vedere în cadrul procesului de auditare. Acestea ar putea fi, pe lângă elaborarea planului de acțiuni, conștientizarea importanței datelor cu caracter personal și responsabilizarea companiei.

Prin raportare la organigramă, raportul de audit ar trebui să conțină o descriere a activității generale a companiei și o delimitare în funcție de anumite procese particulare. Dacă există departamente, se poate avea în vedere și o descriere a activității acestora. Nu toate companiile se comportă la fel în ceea ce privește activitățile interne. De exemplu, întâlnim companii care se ocupă prin intermediul unui departament specializat de relațiile de muncă, inclusiv salarizare, însă pot exista companii care realizează intern partea de încheiere a contractelor de muncă, a recrutării dar care au optat să externalizeze partea de salarizare.

Mai departe, se vor stabili categoriile de date cu caracter personal pe care compania le prelucrează pe fiecare element al unei activități. De exemplu, analizând activitatea departamentului de securitate din cadrul unei companii pe modelul propus, se va putea identifica imaginea persoanelor vizate (salariați și vizitatori), date de geolocalizare cu privire la angajați prin raportare la autovehiculul pus la dispoziție de companie în vederea îndeplinirii atribuțiilor ori pentru a le oferi un avantaj sau după caz, prin raportare la telefonul de serviciu pe care angajatul îl folosește etc. Compania trebuie să identifice și sursa acestor date. În concret, se va stabili pentru fiecare categorie dacă datele provin de la persoana vizată sau din surse externe, iar în măsura în care acestea au fost colectate din alte surse se vor identifica, pe cât posibil, aceste surse.

Raportul de audit va trata inclusiv partea de retenție a datelor, atât pe suport material, cât și electronic și eventualele măsuri deja avute în vedere la nivelul companiei în vederea protejării acestor date precum și accesul la aceste date.

O atenție sporită va fi acordată transferului internațional de date, în special în ceea ce privește propunerea măsurilor în eventualitatea în care se identifică un astfel de transfer fără să fi fost luate măsuri.

PRACTICA AUTORITĂȚILOR

„Cea mai scumpă parte a construcțiilor o reprezintă greșelile”.

Ken Folett

În practică, întâlnim deseori replica „amenzile de rândul zecilor sau sutelor de mii de euro se aplică firmelor mari” sau „ne îndoim de faptul că vor veni chiar la noi”. Ei bine, lucrurile nu stau chiar așa. La o scurtă analiză a cazuisticii existente la nivelul Spațiului Economic European, putem observa faptul că amenzile aplicate nu țin cont de dimensiunile operatorului, sancțiunile aplicate vizând inclusiv persoane fizice care au făcut fotografii ale persoanelor vizate fără a avea un acord din partea acestora sau care au utilizat sisteme de supraveghere video care permiteau înregistrarea inclusiv pe spațiul public.

Analiza sancțiunilor aplicate de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) dar și a celorlalte autorități de supraveghere europene este foarte importantă, operatorii putând „învăța” din „greșelile” altor operatori ce au fost sancționate. Din această rațiune, la analiza punctuală a fiecărui caz, vom identifica aspectele de reținut pe care recomandăm ca operatorii să le trateze cu prioritate în cadrul planurilor de conformare.

Clasamentul autorităților de supraveghere europene în funcție de numărul de sancțiuni aplicate

Autoritatea de supraveghere din România ocupă un loc fruntaș între autoritățile din Europa în ceea ce privește volumul de amenzi aplicate, fiind pe locul 2, cu un număr de peste 30 de amenzi aplicate, imediat după autoritatea de supraveghere spaniolă, care a aplicat peste 100 de amenzi, cu mult peste celelalte autorități din Europa.

Clasamentul autorităților de supraveghere din Spațiul Economic European în funcție de numărul de sancțiuni aplicate³⁰:

³⁰ Conform GDPR Enforcement Tracker: <https://www.enforcementtracker.com/>, la data de 01.08.2020.

1. Spania – 117 sancțiuni (amenzi aplicate în cuantum de peste 3.300.000 de euro);
2. România – 32 sancțiuni (amenzi aplicate în cuantum de peste 500.000 de euro);
3. Ungaria – 28 sancțiuni (amenzi aplicate în cuantum de peste 500.000 de euro);
4. Germania – 26 sancțiuni (amenzi aplicate în cuantum de peste 26.300.000 de euro);
5. Bulgaria – 20 sancțiuni (amenzi aplicate în cuantum de peste 3.300.000 de euro);
6. Italia – 16 sancțiuni (amenzi aplicate în cuantum de peste 57.100.000 de euro);
7. Belgia – 14 sancțiuni (amenzi aplicate în cuantum de peste 700.000 de euro);
8. Cehia – 11 sancțiuni (amenzi aplicate de peste 19.000 de euro);
9. Norvegia – 10 sancțiuni (amenzi aplicate de peste 1.000.000 de euro);
10. Grecia – 9 sancțiuni (amenzi aplicate de peste 700.000 de euro).

Clasamentul autorităților de supraveghere europene prin raportare la cuantumul sancțiunilor aplicate

Locul fruntaș în acest clasament este ocupat de Marea Britanie, care se detașează de toate celelalte autorități de supraveghere europene, dacă ne gândim doar la faptul că trei amenzi aplicate de către ICO UK – autoritatea competentă însumează aproximativ 315.000.000 de euro.

Clasamentul autorităților de supraveghere europene prin raportare la cuantumul sancțiunilor aplicate:

2. Italia (amenzi aplicate în cuantum de peste 57.100.000 de euro – 16 amenzi);
3. Franța (amenzi aplicate de peste 51.100.000 de euro – 5 amenzi);
4. Germania (amenzi aplicate de peste 26.300.000 de euro – 26 amenzi);
5. Austria (amenzi aplicate de peste 18.000.000 de euro – 7 amenzi);
6. Suedia (amenzi aplicate de peste 7.000.000 de euro – 6 amenzi);
7. Olanda (amenzi aplicate de peste 3.400.000 de euro – 6 amenzi);

8. Spania (amenzi aplicate de peste 3.300.000 de euro – 117 amenzi);
9. Bulgaria (amenzi aplicate de peste 3.200.000 de euro – 20 amenzi);
10. Norvegia (amenzi aplicate de peste 1.000.000 de euro – 10 amenzi).

Clasamentul sancțiunilor prin raportare la încălcări

Încălcările frecvent sancționate constau în inexistența unor măsuri tehnice și organizatorice adecvate sau, după caz, în insuficiența acestora, în prelucrarea de date în baza unui temei legal insuficient sau după caz, incorect gestionat de către operatorul de date, în nerespectarea principiilor privind prelucrarea datelor ori ale drepturilor persoanelor vizate, în nerespectarea obligației legale de a notifica autoritatea de supraveghere în cazul unei breșe de securitate ori în lipsa de cooperare cu autoritatea sau în nerespectarea obligației legale de a desemna un DPO.

Încălcările constatate pot fi incluse într-un clasament al aspectelor sancționate, prin raportare la cuantumul amenzilor sau prin raportare la numărul acestora.

Clasamentul sancțiunilor prin raportare la cuantumul amenzilor³¹

1. Insuficiența măsurilor tehnice și organizatorice adecvate (amenzi aplicate în cuantum de peste 330.000.000 de euro);
2. Temei legal insuficient (amenzi aplicate în cuantum de peste 120.000.000 de euro);
3. Nerespectarea principiilor privind prelucrarea datelor (amenzi aplicate de peste 17.000.000 de euro);
4. Nerespectarea drepturilor persoanelor vizate (amenzi aplicate de peste 9.500.000 de euro);
5. Nerespectarea obligației de informare a persoanelor vizate (amenzi aplicate de peste 500.000 de euro);
6. Nerespectarea obligației de notificare a autorității de supraveghere în cazul unei breșe de securitate (amenzi de peste 200.000 de euro);

³¹ *Idem* 1.

7. Lipsa desemnării unui DPO (amenzi de peste 100.000 de euro);
8. Necooperarea cu autoritatea de supraveghere (amenzi de peste 100.000 de euro);
9. Nerespectarea obligației privind încheierea de acorduri de prelucrare;
10. Nerespectarea obligațiilor derivate din breșa de securitate.

Clasamentul sancțiunilor prin raportare la numărul amenzilor³²

1. Temei legal insuficient (peste 130 de amenzi);
2. Insuficiența măsurilor tehnice și organizatorice adecvate (peste 75 de amenzi);
3. Nerespectarea principiilor privind prelucrarea datelor (peste 55 de amenzi);
4. Nerespectarea drepturilor persoanelor vizate (peste 35 de amenzi);
5. Nerespectarea obligației de informare a persoanelor vizate (peste 15 amenzi);
6. Necooperarea cu autoritatea de supraveghere (peste 10 amenzi);
7. Nerespectarea obligației de notificare a autorității de supraveghere în cazul unei breșe de securitate;
8. Lipsa desemnării unui DPO;
9. Nerespectarea obligației privind încheierea de acorduri de prelucrare;
10. Nerespectarea obligațiilor derivate din breșa de securitate.

Analiza măsurilor dispuse de autoritățile de supraveghere

Austria

Autoritatea de supraveghere austriacă a aplicat, până la acest moment, un număr total de 7 amenzi, principalul aspect sancționat constând în insuficiența temeiului legal de prelucrare.

În anul 2020, nu a fost aplicată nicio sancțiune.

În anul 2019, au fost aplicate 3 amenzi pentru nerespectarea GDPR:

- Autoritatea pentru Protecția Datelor (DSB) din Austria a sancționat poșta din Austria cu suma de 18.000.000 de euro, motivul fiind insuficiența temeiului legal pentru prelucrarea datelor.

³² *Idem* 1.

Situația de fapt ce a stat la baza aplicării sancțiunii: Poșta a creat profiluri pentru mai mult de trei milioane de persoane ce includeau inclusiv informații precum adrese personale sau preferințe personale, acestea fiind vândute ulterior către companii și partide politice.



DE REȚINUT! Practica vânzării bazelor de date conținând adrese de e-mail a fost foarte răspândită, inclusiv pe teritoriul României. Deși acum întâlnim foarte rar în practică astfel de situații, recomandăm operatorilor să fie atenți la orice transfer (chiar cu titlu gratuit) al unor informații atât de sensibile colectate pe bază de consimțământ al persoanei vizate (de exemplu, preferințe). Utilizarea unor astfel de date în alte scopuri decât cele pentru care au fost colectate/de către un alt operator poate atrage răspunderea operatorilor implicați.

o Autoritatea pentru Protecția Datelor (DSB) din Austria a aplicat unei companii din sectorul medical amenda de 50.000 de euro pentru îndeplinirea insuficientă a obligației legale de informare și pentru lipsa de desemnare a unui DPO.



DE REȚINUT! Una dintre obligațiile esențiale pe care GDPR le impune companiilor constă în informarea persoanelor vizate. Această informare este necesară chiar și atunci când datele colectate sunt necesare în vederea furnizării serviciului medical. Întâlnim în practică foarte multe situații în care, la nivelul clinicilor medicale, există o serie de formulare din care rezultă că persoana vizată este de acord ca datele sale să fie prelucrate conform cerințelor legale, considerându-se, în mod eronat, că un astfel de formular este de natură să „acopere” societatea în ceea ce privește o eventuală sancțiune rezultată din nerespectarea GDPR. Observăm faptul că datele persoanelor vizate sunt prelucrate cu ajutorul diverselor aplicații, prin intermediul unor call-centere, a unor laboratoare partenere etc, neexistând însă nicio informare a pacienților cu privire la acest aspect, aspect ce poate conduce la sancționarea companiei.

În ceea ce privește desemnarea responsabilului, deși legea nu prevede expres obligativitatea operatorilor din acest domeniu de a desemna un DPO, suntem de părere că necesitatea desemnării acestuia rezultă din faptul că orice clinică medicală prelucrează în mod sistematic date cu caracter personal, inclusiv date sensibile. Recomandăm, așadar, ca orice operator din domeniul medical să desemneze un DPO și să îl

notifice la ANSPDCP, completând formularul specific de pe site-ul autorității ținând cont și de orice eventuale conflicte de interese.

- o Autoritatea pentru Protecția Datelor (DSB) din Austria a sancționat cu amendă în cuantum de 11.000 de euro un antrenor de fotbal, motivul fiind insuficiența temeiului legal pentru prelucrarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Antrenorul a fost amendat deoarece timp de mai mulți ani a filmat mai multe sportive în timp ce erau la dușuri.



DE REȚINUT! Orice profesionist are obligația de a respecta cerințele GDPR. Cunoaștem practica multor antrenori care publică antrenamentele live pe paginile lor de social-media sau ale companiei pe care o reprezintă. În astfel de situații, deși se poate pune problema interesului legitim de a face cât mai cunoscută activitatea sportivă, recomandăm să existe o informare a persoanelor vizate anterior realizării oricărui material și oferirii opțiunii de a nu participa dacă nu se dorește.

În anul 2019, au fost aplicate 4 amenzi pentru nerespectarea GDPR:

- o Autoritatea pentru Protecția Datelor (DSB) din Austria a sancționat cu amendă în cuantum de 2.200 de euro o persoană privată, motivul fiind insuficiența temeiului legal pentru prelucrarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Persoana respectivă folosea sistem de supraveghere video acasă, sistemul acoperind inclusiv zone de interes general din complexul rezidențial, precum parcuri, grădină sau zona de acces în complex, acoperind chiar și o zonă dintr-o proprietate privată adiacentă. Astfel, s-a considerat că supravegherea nu este proporțională cu scopul său și nu se limitează la ce este necesar, fiind și nesemnificativă corespunzător.



DE REȚINUT! Orice persoană care instalează un sistem de supraveghere video se va asigura de faptul că sistemul este semnalizat corespunzător cu pictograme specifice și nu permite înregistrarea pe spațiul public ori pe proprietățile vecine.

- o Autoritatea pentru Protecția Datelor (DSB) din Austria a sancționat cu amendă de 4.800 de euro o casă de pariuri, motivul fiind neîndeplinirea obligației de informare a persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Supravegherea video nu era suficient semnalizată, fiind înregistrată o parte considerabilă din trotuar – spațiul public.



DE REȚINUT! Companiile care utilizează sisteme de supraveghere video vor limita înregistrările camerelor strict la spațiul în care se desfășoară activitate și la proprietatea deținută/închiriată.

- o Autoritatea pentru Protecția Datelor (DSB) din Austria a sancționat cu amendă în cuantum de 300 de euro posesorul unui autoturism, motivul fiind insuficiența temeiului legal pentru prelucrarea datelor, camera de bord fiind utilizată în scopuri nelegale.



DE REȚINUT! Discuțiile privind legalitatea camerelor auto sunt ample, acestea înregistrând, cel mai adesea, spațiile publice. Cu toate acestea, recomandăm ca posesorii de autoturisme în care sunt instalate camere de bord să se limiteze în utilizarea camerei la ceea ce este necesar (utilizare imagini strict în cazul unui accident, ștergerea de îndată a imaginilor care nu sunt necesare etc.).

- o Autoritatea pentru Protecția Datelor (DSB) din Austria a sancționat cu amendă în cuantum de 1800 de euro un restaurant, motivul fiind insuficiența temeiului legal pentru prelucrarea datelor, neîndeplinirea obligației de a informa persoanele vizate, precum și nerespectarea principiului minimizării, imaginile fiind stocate pentru o perioadă de 14 zile.



DE REȚINUT! Companiile care utilizează sisteme de supraveghere video se vor asigura, faptul că acestea sunt semnalizate corespunzător prin intermediul pictogramelor specifice și se vor asigura că durata de retenție este proporțională scopului în care sistemul a fost instalat.

Belgia

Autoritatea de supraveghere belgiană a aplicat, până la acest moment, un număr total de 14 amenzi, principalele aspecte sancționate constând în insuficiența temeiului legal de prelucrare și în nerespectarea drepturilor persoanelor vizate.

În anul 2020, au fost aplicate 8 amenzi pentru nerespectarea GDPR:

- o Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat cu amendă în cuantum de 600.000 de euro operatorul Google Belgium SA, motivul fiind insuficiența temeiului legal pentru prelucrarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: O persoană vizată a solicitat companiei să elimine o serie de articole cu privire la preținse fapte de hărțuire ce îi afectau reputația. Sancțiunea a vizat respingerea cererii persoanei vizate de către Google Belgium SA.



DE REȚINUT! Conform CJUE, operatorul unui motor de căutare pe internet răspunde pentru prelucrarea pe care o efectuează în ceea ce privește datele cu caracter personal care apar pe pagini web publicate de terți.

- o Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat cu amendă în cuantum de 5.000 de euro un operator al unui sistem de supraveghere video din cadrul unei clădiri rezidențiale, motivat de insuficiența temeiului legal pentru prelucrarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Persoana în cauză a instalat sistemul de supraveghere video pentru a monitoriza aria comună a două blocuri de apartamente. Operatorul a argumentat măsura ca având la bază consimțământul persoanelor vizate exprimat prin intermediul contractului de vânzare-cumpărare.



DE REȚINUT! Un consimțământ exprimat prin intermediul unui contract, fiind inclus între clauzele acestuia, poate fi considerat ca fiind nevalid de către autoritatea de supraveghere. Un astfel de acord trebuie să îndeplinească toate condițiile prevăzute de GDPR pentru consimțământ. Un astfel de consimțământ ar putea fi considerat ca fiind condiționat în anumite situații, deoarece neoferirea acestuia ar putea conduce, uneori, la încheierea contractului.

- o Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat o companie cu amendă în cuantum de 10.000 de euro, motivat de nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania respectivă a trimis un e-mail fără acordul destinatarului, motiv pentru care acesta a solicitat informații referitoare la intrările în baza de date referitoare la persoana respectivă, fără a primi un răspuns.



DE REȚINUT! Compania are obligația, conform GDPR, să ofere răspunsuri pentru solicitările persoanelor vizate în termen de cel mult

o lună de la primirea cererii. Doar în cazuri justificate poate opera o extindere a acestui termen.

- o Autoritatea pentru Protecția Datelor (APD) din Belgia a aplicat o amendă în valoare de 1.000 de euro, motivat de nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Persoana vizată a primit în repetate rânduri e-mailuri cu reclame ale unei companii, deși a obiectat la prelucrarea datelor sale și a solicitat ștergerea lor, iar compania nu a răspuns acestor cerințe.



DE REȚINUT! Compania are obligația, conform GDPR, să ofere răspunsuri pentru solicitările persoanelor vizate în termen de cel mult o lună de la primirea cererii.

- o Autoritatea pentru Protecția Datelor (APD) din Belgia a aplicat o amendă în cuantum de 5.000 de euro unui angajat municipal, motivat de insuficiența temeiului de prelucrare a datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: În contextul unor alegeri din 2018, operatorul de date a transmis reclame electorale unui grup de angajați din aceeași administrație, utilizând nelegal o listă de date de contact la care nu avea acces.



DE REȚINUT! Accesarea neautorizată a datelor cu caracter personal poate atrage răspunderea companiei, fiind esențială instruirea angajaților care intră în contact cu datele aparținând operatorului.

- o Autoritatea pentru Protecția Datelor (APD) din Belgia a aplicat o amendă în valoare de 1.000 de euro unui ONG, motivat de nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată, deoarece ONG-ul respectiv a trimis mesaje de marketing, deși persoanele implicate au obiectat la prelucrarea datelor și au optat pentru ștergerea acestora. ONG-ul a invocat ca temei legal pentru prelucrare interesele legitime, nu consimțământul explicit al persoanelor vizate, apărare care nu a fost acceptată de către autoritatea de supraveghere.

- o Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat cu amendă în cuantum de 50.000 de euro un furnizor de social media, motivul fiind insuficiența temeiului de prelucrare a datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania respectivă a trimis invitații unor contacte încărcate de către utilizatori fără consimțământul lor sau orice alt temei legal.



DE REȚINUT! Una dintre cele mai frecvente probleme întâlnite în practică constă în lipsa consimțământului în cadrul prelucrărilor în scopuri de marketing direct. Sigur că operatorul poate lua în calcul și prelucrările de date în scopuri de marketing efectuate în interes legitim, însă doar în acele situații în care există o relație relevantă între operator și persoana vizată (client) și există așteptarea rezonabilă să se comunice astfel de mesaje de către operator.

o Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat cu amendă în cuantum de 50.000 de euro operatorul Proximus SA, motivul fiind lipsa unui DPO.

Situația de fapt ce a stat la baza aplicării sancțiunii: DPO-ul nu era suficient de implicat în procesele interne de prelucrare de date personale și compania nu dispunea de un sistem de prevenire a conflictului de interese în ceea ce îl privea pe responsabil, ocupând numeroase funcții în cadrul acesteia, motiv pentru care autoritatea a ajuns la concluzia că DPO-ul nu putea lucra independent.



DE REȚINUT! Conform cerințelor legale, DPO-ul trebuie să fie independent, fiind absolut necesar să se evite orice conflict de interese. Funcții precum HR manager/responsabil resurse umane, Director Financiar, Director Departament Juridic ar putea fi incompatibile cu cea de DPO. Când există riscul unor astfel de conflicte de interese, operatorul poate opta pentru un DPO externalizat, dar care să se implice în mod activ în activitatea companiei.

În anul 2019, au fost aplicate 6 amenzi pentru nerespectarea GDPR:

o Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat cu amendă în cuantum de 2.000 de euro o organizație de îngrijiri medicale, motivat de nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Organizația nu a dat curs cererilor persoanelor vizate de a oferi acces la date și de a șterge datele.



DE REȚINUT! Compania este obligată să ofere un răspuns solicitărilor persoanelor vizate în termen de cel mult o lună de la primirea solicitărilor. Un eventual refuz de a da curs cererii persoanei vizate trebuie justificat.

○ Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat cu amendă în cuantum de 15.000 de euro un website ce oferea servicii legale, din cauza îndeplinirii insuficiente a obligațiilor de informare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Politica de confidențialitate era disponibilă doar în limba engleză, deși era adresată unui public vorbitor de franceză și germană. Mai mult decât atât, forma inițială a politicii de confidențialitate nu era ușor accesibilă și nu menționa temeiul legal al prelucrării.



DE REȚINUT! Compania va avea în vedere traducerea politicilor de pe site dacă activează pe teritoriul mai multor state și completarea acestor documente prin raportare la anumite cerințe specifice din legislațiile naționale.

○ Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat un primar cu o amendă în cuantum de 5.000 de euro, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată din cauza faptului că au fost trimise e-mailuri electorale pe o serie de adrese de e-mail colectate în alt scop.



DE REȚINUT! Compania nu va utiliza datele în scopuri diferite față de cele cunoscute de persoana vizată. De exemplu, societatea nu va transmite newslettere către adresele de e-mail furnizate de clienți în vederea confirmării unei comenzi online.

○ Autoritatea pentru Protecția Datelor (APD) din Belgia a aplicat o amendă în cuantum de 10.000 de euro unui comerciant, motivul fiind nerespectarea principiilor generale de prelucrare a datelor personale.

Situația de fapt ce a stat la baza aplicării sancțiunii: Comerciantul voia să utilizeze o carte de identitate electronică pentru a crea un card de client. Investigația autorității de supraveghere a relevat faptul că acel comerciant a cerut acces la datele personale de pe cartea de identitate electronică, inclusiv poza și codul de bare aferent codului numeric personal al persoanei vizate.



DE REȚINUT! Companiile vor avea în vedere să instruiască angajații astfel încât să nu solicite pentru stocare/simplă consultare date care nu sunt necesare prelucrărilor de date.

o Autoritatea pentru Protecția Datelor (APD) din Belgia a sancționat un primar cu o amendă în cuantum de 2.000 de euro, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a venit ca urmare a folosirii incorecte a datelor personale de către primar pentru o campanie electorală.



DE REȚINUT! Compania nu va utiliza datele în scopuri diferite față de cele cunoscute de persoana vizată.

Bulgaria

Autoritatea de supraveghere bulgară a aplicat, până la acest moment, un număr total de 20 de amenzi, principalul aspect sancționat constând în insuficiența temeiului legal de prelucrare.

În anul 2020, au fost aplicate 4 amenzi pentru nerespectarea GDPR:

o Autoritatea de supraveghere bulgară (KZLD) a aplicat o amendă în cuantum de 2.000 de euro unui partid politic, motivat de insuficiența temeiului de prelucrare a datelor,

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată pentru falsificarea semnăturilor pe listele de alegători.



DE REȚINUT! În cadrul proceselor de prelucrări de date, operatorii se vor asigura de legalitatea proceselor de prelucrare.

o Autoritatea de supraveghere bulgară (KZLD) a aplicat o amendă în cuantum de 2.560 de euro companiei T.K. EOOD, din cauza insuficienței măsurilor tehnice și organizaționale pentru securitatea informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată pentru prelucrarea nelegală a datelor personale, compania nereușind să adopte măsurile tehnice și organizatorice adecvate pentru securitatea informației. Compania a prelucrat nelegal datele personale ale persoanei vizate reclamante de nouă ori în decurs de 5 luni, încălcările cauzând prejudicii persoanei vizate.



DE REȚINUT! Simpla depunere a unei sesizări de către persoana vizată la autoritatea de supraveghere competentă nu înlătură

dreptul acesteia de a se îndrepta împotriva operatorului pentru prejudiciile cauzate în instanță.

- o Autoritatea de supraveghere bulgară (KZLD) a sancționat cu amendă în cuantum de 2.560 de euro compania L.E. EOOD, din cauza insuficienței măsurilor tehnice și organizaționale pentru securitatea informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Sancțiunea a venit ca urmare a prelucrării nelegale a datelor personale ale persoanei vizate, fără cunoștința și consimțământul acesteia și fără o relație contractuală validă. Datele personale ale persoanei vizate au fost prelucrate nelegal timp de 3 luni din lipsa adoptării măsurilor tehnice și organizatorice necesare pentru asigurarea securității informațiilor.



DE REȚINUT! Pentru preîntâmpinarea unor prelucrări nelegale de date personale, compania trebuie să utilizeze o rețea sigură. Sigur că pot interveni breșe de securitate, chiar dacă societatea îndeplinește condițiile optime în ceea ce privește componenta tehnică, de aceea trebuie avută în vedere instruirea periodică a persoanelor vizate, actualizarea datelor din toate sistemele, implicarea activă a DPO-ului etc.

- o Autoritatea de supraveghere bulgară (KZLD) a sancționat cu amendă de 5.110 euro o companie ce furnizează servicii de utilități.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată pentru prelucrarea nelegală a datelor persoanei vizate. Acestea au fost utilizate pentru întocmirea unui caz împotriva sa pentru nerespectarea obligațiilor de plată. A fost vizat de prelucrarea nelegală salariul acelei persoane, acesteia fiindu-i cauzat un prejudiciu.



DE REȚINUT! O atenție sporită trebuie acordată de angajatori în ceea ce privește popririle asupra drepturilor salariale. De regulă, există comunicări între societate și diverși executori în cadrul cărora se furnizează date privind salariile/bonusurile etc. Compania va depune toate diligențele pentru asigurarea confidențialității acestor date.

În anul 2019, au fost aplicate 15 amenzi pentru nerespectarea GDPR:

- o Autoritatea de supraveghere bulgară (KZLD) a aplicat o amendă în cuantum de 511 euro unui angajator, motivul fiind nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată urmare a faptului că angajatorul refuza să acorde accesul la datele personale pentru angajații care au trimis cereri de acces.



DE REȚINUT! Compania va ține cont de faptul că angajații au calitatea de persoane vizate și va da curs cererilor acestora derivate din procesele de prelucrări. Există companii care au implementat proceduri simplificate pentru exercitarea drepturilor propriilor angajați, pentru o gestionare eficientă a acestora.

o Autoritatea de supraveghere bulgară (KZLD) a sancționat cu o amendă în cuantum de 5.112 euro Ministerul Afacerilor Interne, motivat de insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Ministerul Afacerilor Interne a prelucrat în mod nelegal date personale și a transmis aceste date Republicii Togo.

DE REȚINUT! Inclusiv autoritățile de stat au calitatea de operatori de date, având aceleași obligații de a respecta temeiurile legale de prelucrare a datelor. La nivelul României au fost aplicate sancțiuni autorităților publice în materie de protecție a datelor.

o Autoritatea de supraveghere bulgară (KZLD) a sancționat cu amendă în cuantum de 28.100 de euro Agenția Națională de Venituri, motivat de insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Agenția a prelucrat nelegal datele unei persoane vizate și le-a folosit pentru a începe o executare silită împotriva acesteia pentru recuperarea unei sume de bani. Agenția a colectat și date suplimentare despre conturile sale bancare din registrul Băncii Naționale a Bulgariei, date suplimentare nelegal prelucrate, de asemenea.



DE REȚINUT! Inclusiv autoritățile de stat au calitatea de operatori de date, având aceleași obligații de a respecta temeiurile legale de prelucrare a datelor.

o Autoritatea de supraveghere bulgară (KZLD) a sancționat un furnizor de servicii de telecomunicații cu amenzi în cuantum de 1.022 de euro și 5.113 euro, motivat de insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Datele personale au fost prelucrate pentru încheierea unor contracte de servicii fără cunoștința sau consimțământul persoanelor vizate. Sancțiunile au fost impuse atât furnizorului, cât și reprezentanței din Bulgaria, pentru prelucrarea nelegală a datelor personale.



DE REȚINUT! Există situații în care contractele pot fi încheiate la distanță (electronic sau telefonic), caz în care operatorii vor depune toate diligențele pentru a face dovada consimțământului persoanelor vizate.

- o Autoritatea de supraveghere bulgară (KZLD) a sancționat o reprezentanță comercială a unui furnizor de servicii de telecomunicații cu amendă în cuantum de 11.760 de euro, motivat de insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Reprezentanța a prelucrat în mod nelegal datele persoanei vizate pentru a încheia un contract pentru servicii mobile și un contract de leasing.



DE REȚINUT! Compania se va asigura că utilizează datele persoanele colectate strict în scopul/scopurile pentru care a obținut acordul persoanei vizate.

- o Autoritatea de supraveghere bulgară (KZLD) a sancționat un executor cu o amendă în cuantum de 1.121 de euro, motivat de nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Executorul prelucra date ale persoanei vizate prin mijloace de supraveghere video. Persoana vizată a solicitat acces la date, neprimind răspuns din partea executorului.



DE REȚINUT! Orice prelucrare efectuată de către un operator de date îi conferă persoanei vizate dreptul de acces la aceste informații. Fie că ne referim la înregistrări audio-video, la simple capturi foto ale persoanei vizate sau la un simplu nume colectat în vederea completării unui registru, există obligația entității care colectează să ofere ulterior acces la date.

- o Autoritatea de supraveghere bulgară (KZLD) a sancționat cu amendă în cuantum de 2.600.000 de euro Agenția Națională de Venituri, din cauza insuficienței măsurilor tehnice și organizatorice pentru asigurarea securității informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: A avut loc o scurgere de date personale în urma unui atac cibernetic, cauzat de metodele nepotrivite de securitate a informației. Astfel, datele a aproximativ 6 milioane de persoane au fost accesate ilegal.



DE REȚINUT! Având în vedere volumul foarte mare de date pe care autoritățile publice îl prelucrează, se recomandă ca operatorii din acest segment să trateze cu prioritate partea de securitate a informației.

o Autoritatea de supraveghere bulgară (KZLD) a sancționat DSK Bank cu amendă în cuantum de 511.000 de euro pe motivul măsurilor tehnice și organizatorice insuficiente pentru securitatea informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Lipsa unor măsuri tehnice și organizatorice adecvate pentru securitatea informației a condus la scurgerea datelor personale. Terții au avut acces la peste 23000 de înregistrări de credit referitoare la peste 33000 de clienți ai băncii, inclusiv date precum nume, cetățenie, CNP sau date biometrice.



DE REȚINUT! Băncile, la rândul lor, prelucrează un volum foarte mare de date personal, motiv pentru care se recomandă prioritizarea implementării de măsuri tehnice adecvate care să asigure securitatea informației.

o Autoritatea de supraveghere bulgară (KZLD) a sancționat cu o amendă de 511 euro o serie de centre medicale, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Centrele medicale utilizau un software pentru a genera un formular pentru schimbarea medicului persoanelor vizate, formularul fiind trimis Fondului Regional pentru Asigurări de Sănătate și altui centru medical, ceea ce a dus ulterior la prelucrarea nelegală a datelor.



DE REȚINUT! Transferurile de date între partenerii unui lanț medical nu pleacă de la prezumția de nelegalitate. Operatorii care efectuează astfel de prelucrări trebuie să se asigure că sunt implementate măsuri tehnice și organizatorice adecvate pentru toți partenerii către care se efectuează transferuri.

o Autoritatea de supraveghere bulgară (KZLD) a sancționat cu amendă în cuantum de 5.100 de euro compania A.P. EOOD, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea a prelucrat nelegal datele persoanei vizate, acestea fiind utilizate pentru pregătirea unui contract de muncă, în timp ce aceasta se afla în închisoare.



DE REȚINUT! Compania se va asigura de faptul că poate demonstra în orice moment existența unui consimțământ sau, după caz, aplicabilitatea unui temei de prelucrare.

○ Autoritatea de supraveghere bulgară (KZLD) a sancționat cu amendă în cuantum de 27.100 de euro un furnizor de servicii de telecomunicații, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au avut loc înregistrări repetate pentru anumite servicii, fără cunoștința și consimțământul persoanei vizate care ar fi trebuit să solicite înregistrarea. Angajații furnizorului de servicii au utilizat datele personale și au înregistrat presupusele solicitări pentru serviciile respective. Persoana vizată nu a semnat niciun formular și nu a consimțit la prelucrarea datelor în acel scop. Semnătura reclamantului nu corespundea cu semnătura de pe formular. Deși CNP-ul persoanei era trecut, numărul cărții de identitate era diferit.



DE REȚINUT! Compania se va asigura de faptul că poate demonstra în orice moment existența unui consimțământ sau, după caz, aplicabilitatea unui alt temei de prelucrare.

○ Autoritatea de supraveghere bulgară (KZLD) a aplicat o amendă în cuantum de 500 de euro unui angajator, motivat de nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un angajat a cerut acces la datele sale personale, dar nu a primit un răspuns complet și în timp util.



DE REȚINUT! Având în vedere calitatea de persoană vizată a salariatului, angajatorul va oferi răspunsuri solicitărilor acestuia privind exercitarea drepturilor sale legale, chiar dacă acest răspuns ar putea fi negativ (de exemplu, solicitarea privind ștergerea datelor aferente contractului de muncă va fi respinsă, din moment ce angajatorul are obligația legală de a prelucra acele date chiar și după încetarea relației de muncă).

○ Autoritatea de supraveghere bulgară (KZLD) a aplicat o amendă în cuantum de 500 de euro unei bănci, motivat de insuficiența temeiului legal pentru prelucrarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Banca a obținut date privind un student fără a avea temei legal.



DE REȚINUT! Compania se va asigura de faptul că poate demonstra în orice moment aplicabilitatea unui temei de prelucrare.

În anul 2018, au fost aplicată o singură amendă pentru nerespectarea GDPR:

- o Autoritatea de supraveghere bulgară (KZLD) a aplicat o amendă de 500 de euro unei bănci, motivat de insuficiența temeiului legal pentru prelucrarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Banca a fost amendată, pentru că a contactat telefonic un client pentru facturile neachitate ale unui vecin, iar clientul a invocat dreptul de a fi uitat. Inițial nu a primit răspuns la cerere, motiv pentru care a mai formulat una.



DE REȚINUT! Compania va lua legătura direct cu persoanele vizate în cazul în care există debite de plată aferente unui contract în derulare sau încetat.

Croația

- o Autoritatea de supraveghere croată (azop) a aplicat o singură amendă pentru nerespectarea GDPR, în anul 2020, motivul fiind nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: În perioada mai 2018 – aprilie 2019, o bancă a refuzat să pună la dispoziția clienților copii de pe documentele referitoare la credit. Aceasta a insistat asupra faptului că acele documente nu intrau sub incidența dreptului de acces. A fost inițiată o procedură pe baza plângerilor, iar autoritatea de supraveghere a impus băncii să respecte dreptul de acces și să pună la dispoziție documentele solicitate. Autoritatea a luat în considerare faptul că banca nu a respectat măsurile impuse, a continuat acea practică timp de aproape un an, negând dreptul la acces pentru mai mult de 2500 de clienți.



DE REȚINUT! Atunci când o persoană vizată transmite o cerere de acces la date, compania va răspunde solicitării în termen de cel mult o lună de la date depunerii.

Cipru

Autoritatea de supraveghere cipriotă a aplicat, până la acest moment, un număr total de 8 amenzi, principalul aspect sancționat constând în insuficiența temeiului legal de prelucrare.

În anul 2020, au fost aplicate 2 amenzi pentru nerespectarea GDPR:

- o Autoritatea de supraveghere cipriotă a aplicat o amendă în cuantum de 9.000 de euro Serviciilor de asigurări sociale ale Ministerului Muncii, Asistenței Sociale și Asigurărilor Sociale, din cauza măsurilor tehnice și organizatorice de securizare a informației insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Poliției i-a fost acordat accesul la date personale și nu au fost luate măsuri de securitate a datelor, în ciuda atenționărilor în acest sens din partea autorității.



DE REȚINUT! Există multe practici în baza cărora autoritățile transmit date personale fără a exista un consimțământ sau o informare a persoanelor vizate cu privire la aceste transferuri de date. Mai mult decât atât, există și protocoale încheiate de autorități care prevăd astfel de transferuri, a căror legalitate este discutabilă.

- o Autoritatea de supraveghere cipriotă a aplicat o amendă în cuantum de 1.000 de euro unui magazin online, motivat de insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost trimise fără consimțământ mesaje în scop de marketing. Nu au fost luate măsuri adecvate, cum ar fi posibilitatea proprietarilor telefoanelor de a bloca mesajele de marketing.



DE REȚINUT! Pot exista situații în care mesajele de marketing pot fi transmise fără consimțământ, marketingul direct putând fi corelat cu interesele legitime ale unei companii. Un astfel de interes legitim ar putea exista atunci când există o relație relevantă între companie și persoana vizată (persoana vizată are un cont pe platforma respectivă) și există așteptări rezonabile din partea persoanei vizate cu privire la primirea acestor comunicări de marketing.

În anul 2019, au fost aplicate 6 amenzi pentru nerespectarea GDPR:

- o Autoritatea de supraveghere cipriotă a aplicat trei amenzi companiilor LGS Handling Ltd, Louis Travel Ltd și Louis Aviation Ltd,

motivată de insuficiența temeiului de prelucrare. Amenzile au fost în cuantum de 70.000 de euro, 10.000 de euro, respectiv 2.000 de euro.

Situația de fapt ce a stat la baza aplicării sancțiunilor: S-a constatat că utilizarea factorului Bradford pentru profilarea și monitorizarea concediilor medicale a reprezentat o prelucrare ilegală a datelor cu caracter personal.



DE REȚINUT! În cadrul prelucrărilor de date, compania va identifica cele mai puțin intruzive mijloace de prelucrare, mai ales în relațiile de muncă, acolo unde se prezumă că angajatul nu își poate exprima dezacordul cu privire la astfel de măsuri, dat fiind raportul de subordonare.

o Autoritatea de supraveghere cipriotă a dispus sancționarea unui spital de stat pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un pacient a depus plângere la autoritatea de supraveghere, deoarece nu i s-a acordat acces la dosarul său medical de către spital pe motiv că operatorul nu putea identifica dosarul.



DE REȚINUT! Operatorul, fie că este din sectorul privat, fie că este din sectorul public, este obligat să prevină orice incidente (pierdere, ștergere, distrugere etc.) cu privire la datele pe care le deține.

o Autoritatea de supraveghere cipriotă a aplicat o amendă în cuantum de 10.000 de euro pentru o publicație, motivată de insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: În ziar, atât online cât și fizic, au fost făcute publice fotografiile unor anchetatori împreună cu alte informații care conduceau la identificarea acestor persoane. Autoritatea a constatat faptul că se puteau folosi doar inițialele numelor, puteau fi făcute neclare fețele sau puteau fi făcute fotografii de la distanță, care să nu permită identificarea persoanelor.



DE REȚINUT! Libertatea de exprimare în ceea ce privește astfel de publicații nu exonerează operatorul de responsabilitate în materie de protecție a datelor.

o Autoritatea de supraveghere cipriotă a dispus sancționarea unui medic cu amendă de 14.000 de euro, motivată de insuficiența temeiului legal de prelucrare a datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un pacient a formulat o plângere, conform căreia nu i s-a acordat acces la dosarul său medical, explicația oferită fiind aceea că dosarul nu a putut fi găsit.



DE REȚINUT! Operatorul, fie că este din sectorul privat, fie că este din sectorul public, este obligat să prevină orice incidente (pierdere, ștergere, distrugere etc.) cu privire la datele pe care le deține.

Cehia

Autoritatea de supraveghere cehă a aplicat, până la acest moment, un număr total de 11 amenzi, principalele aspecte sancționate constând în insuficiența temeiului legal de prelucrare și în nerespectarea drepturilor persoanelor vizate.

În anul 2020, nu a fost aplicată nicio amendă pentru nerespectarea GDPR.

În anul 2019, au fost aplicate 6 amenzi:

- o Autoritatea de supraveghere cehă (UOOU) a dispus o amendă de 194 de euro, motivat de nerespectarea drepturilor persoanelor vizate. Alte detalii nu sunt cunoscute.

- o Autoritatea de supraveghere cehă (UOOU) a dispus o amendă de 10.000 de euro pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Prelucrarea nu a fost limitată doar la ce era necesar pentru scopul prelucrării și datele nu au fost păstrate astfel încât să permită identificarea doar pentru cât este necesar pentru scopurile prelucrării.



DE REȚINUT! Compania trebuie să se asigure că se limitează strict la datele necesare prelucrării. O măsură organizatorică care poate da eficiență principiului minimizării este fluxul de date care conduce la identificarea tuturor categoriilor de date prelucrate și implicit, la eliminarea celor care nu sunt necesare prelucrării.

- o Autoritatea de supraveghere cehă (UOOU) a sancționat cu amendă în cuantum de 776 de euro un operator pentru nerespectarea drepturilor persoanelor vizate.



DE REȚINUT! Orice operator, fie că face parte din sectorul privat, fie că face parte din sectorul public, va acorda o importanță sporită exercitării drepturilor persoanelor vizate.

o Autoritatea de supraveghere cehă (UOOU) a sancționat cu amendă în cuantum de 1.165 de euro o companie de închirieri auto, pentru îndeplinirea insuficientă a obligațiilor de informare.

Situația de fapt ce a stat la baza aplicării sancțiunii: O persoană care a închiriat o mașină a descoperit faptul că aceasta era urmărită prin GPS de către compania de la care a închiriat-o, deși nu a fost informată în acest sens.



DE REȚINUT! Operatorul are obligația de a informa persoanele vizate – șoferii mașinilor cu privire la mijloacele de geolocalizare existente în autovehiculul pus la dispoziție. Fie că persoana vizată este un client care închiriază mașina, fie că aceasta este un salariat care utilizează o mașină de serviciu, obligatorul are obligația de a informa persoana în cauză cu privire la existența mijlocului GPS.

o Autoritatea de supraveghere cehă (UOOU) a sancționat un broker de credite cu amendă în cuantum de 1.165 de euro din cauza măsurilor tehnice și organizatorice pentru asigurarea securității informației insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Datele nu au fost prelucrate într-un mod care să asigure o protecție optimă, inclusiv împotriva prelucrării nelegale și neautorizate și împotriva pierderilor, distrugerilor accidentale.



DE REȚINUT! Operatorul, fie că este din sectorul privat, fie că este din sectorul public, este obligat să prevină orice incidente (pierdere, ștergere, distrugere etc.) cu privire la datele pe care le deține.

o Autoritatea de supraveghere cehă (UOOU) a aplicat o amendă în cuantum de 388 de euro unui angajator, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un fost angajat al companiei a solicitat ștergerea informațiilor referitoare la persoana sa ce fuseseră publicate pe pagina de Facebook a angajatorului și care au rămas disponibile cu mult după încetarea relației de muncă.



DE REȚINUT! Publicarea pe pagina de Facebook a pozelor de echipă sau a pozelor individuale cu membrii ai echipei are la bază interesele legitime ale operatorului. Având în vedere faptul că există riscul ca pe pagina de social-media să apară fotografii ale persoanelor cu mult timp după încetarea relației de muncă, se recomandă ca în cadrul companiei să fie desemnat un responsabil/mai mulți responsabili care să șteargă la anumite intervale de timp, fotografiile cu angajații sau foștii angajați.

În anul 2018, au fost aplicate 4 amenzi pentru nerespectarea GDPR:

- o Autoritatea de supraveghere cehă (UOOU) a dispus sancționarea cu amendă în cuantum de 388 de euro, motivat de nerespectarea drepturilor persoanelor vizate.

- o Autoritatea de supraveghere cehă (UOOU) a sancționat UniCredit Bank Czech Republic and Slovakia cu amendă în cuantum de 3.140 de euro, motivat de insuficiența temeiului pentru prelucrarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Banca a creat un cont bancar personal pentru o persoană vizată, fără consimțământul său. De asemenea, nu a putut fi dovedită relația contractuală dintre bancă și persoana vizată.



DE REȚINUT! Operatorul trebuie să poată face dovada obținerii consimțământului persoanei vizate sau a oricărui alt temei de prelucrare aplicabil.

- o Autoritatea de supraveghere cehă (UOOU) a dispus sancționarea operatorului Alza.cz cu amendă în cuantum de 588 de euro, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a obținut o copie de pe cartea de identitate a persoanei vizate cu consimțământul său, dar nu a reacționat când acesta și l-a retras și a continuat să prelucreze datele.



DE REȚINUT! În cazul retragerii consimțământului persoanei vizate, în măsura în care nu mai există alt temei de prelucrare aplicabil, operatorul va înceta orice proces de prelucrare.

- o Autoritatea de supraveghere cehă (UOOU) a sancționat cu amendă un antreprenor cu suma de 980 de euro din cauza măsurilor tehnice și organizatorice insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Deținătorul unui joc online a fost expus unor atacuri informatice care au cauzat o funcționare precară a serverelor. De asemenea, operatorul a fost șantajat să plătească o anumită sumă de bani pentru ca atacurile să înceteze. Ca parte a șantajului, hacker-ul s-a oferit să îmbunătățească protecția serverelor operatorului, propunere acceptată de acesta. Astfel, operatorul a implementat noul cod care era mai bun, dar acesta a oferit atacatorului posibilitatea să fure toate datele de pe server referitoare la jucători și să le posteze pe site-ul său. Din acest motiv, autoritatea de supraveghere a ajuns la concluzia că operatorul nu a luat măsurile de siguranță necesare.



DE REȚINUT! În cazul în care intervine un astfel de atac informatic, operatorul trebuie să ia în calcul obligațiile legale ce îi revin în materie de breșe de securitate.

Danemarca

Autoritatea de supraveghere daneză a aplicat, până la acest moment, un număr total de 7 amenzi, principalul aspect sancționat constând în nerespectarea principiilor prelucrării prevăzute de GDPR.

În anul 2020 au fost aplicate 5 amenzi pentru nerespectarea GDPR:

- o Autoritatea de supraveghere daneză (Datatilsynet) a aplicat o amendă în cuantum de 147.800 de euro operatorului rp-Hansen Hotel Group A/S, motivul fiind nerespectarea principiilor prelucrării.

Situația de fapt ce a stat la baza aplicării sancțiunii: În timpul unei investigații, autoritatea daneză a verificat sistemele IT ale operatorului pentru a verifica dacă sunt implementate suficiente proceduri care să asigure păstrarea datelor pentru o durată determinată, nu mai lungă decât cea necesară scopului în care acestea au fost colectate. A rezultat faptul că operatorul avea date pentru care expirate durata de retenție, durată stabilită chiar de către operator.



DE REȚINUT! Un aspect foarte important de care companiile trebuie să țină cont este durata de retenție, atât cea impusă prin diverse acte normative, cât și cea stabilită intern, prin intermediul propriilor proceduri implementate în cadrul proceselor de conformare.

o Autoritatea de supraveghere daneză (Datatilsynet) a sancționat Municipiul Lejre cu amendă în cuantum de 6.700 de euro, din cauza nerespectării principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Autoritatea de supraveghere a descoperit faptul că Municipiul Lejre și Centrul pentru Tineret au postat regulat pe portalul personalului Municipiului Lejre minute ale ședințelor cu date personale, inclusiv ale unor cetățeni sub 18 ani, acestea fiind accesibile angajaților municipiului, indiferent dacă aceștia aveau sarcini ce priveau acele date sau nu.



DE REȚINUT! Accesul nepermis la datele personale poate atrage răspunderea operatorului, considerându-se că nu au fost implementate măsuri adecvate.

o Autoritatea de supraveghere daneză (Datatilsynet) a dispus sancționarea operatorului JobTeam A/S DKK cu amendă în cuantum de 6.700 de euro pentru nerespectarea drepturilor persoanei vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a șters fără o bază legală datele personale ce erau subiectul unei cereri de acces.



DE REȚINUT! Se recomandă ca în cazul unei cereri de acces să nu se procedeze la ștergerea datelor ce fac obiectul solicitării persoanei vizate, o astfel de conduită putând conduce la sancționarea operatorului.

o Autoritatea de supraveghere daneză (Datatilsynet) a aplicat o amendă în cuantum de 7.000 de euro Municipiului Hørsholm, motivat de insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Calculatorul unui angajat al autorității locale a fost furat, acesta conținând datele personale a aproximativ 1600 de angajați ai autorității locale, inclusiv informații sensibile.



DE REȚINUT! Operatorul depune toate diligențele pentru a preîntâmpina incidentele de securitate precum furt, pierdere etc.

o Autoritatea de supraveghere daneză (Datatilsynet) a aplicat o amendă în cuantum de 14.000 de euro Municipiului Gladsaxe din cauza insuficienței măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un calculator din cadrul autorității care nu era protejat prin criptare a fost furat, incluzând informații sensibile și CNP-uri ale 20 620 de rezidenți ai orașului.



DE REȚINUT! Riscurile în cazul incidentelor de securitate se reduc semnificativ dacă există măsuri tehnice care să asigure securitatea informației (de exemplu, criptare).

În anul 2019 au fost aplicate 2 amenzi pentru nerespectarea GDPR:

- o Autoritatea de supraveghere daneză (Datatilsynet) a aplicat o amendă în cuantum de 200.850 de euro operatorului IDdesign A / S pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a prelucrat datele personale a aproximativ 385 000 clienți pentru o perioadă mai lungă decât cea necesară prelucrării. În plus, compania nu a stabilit un termen pentru ștergerea datelor în noul sistem de management al relațiilor cu clienții. De asemenea, termenele vechi nu au fost respectate atunci când s-au împlinit.



DE REȚINUT! Operatorul este ținut să respecte duratele de retenție stabilite prin acte normative sau, după caz, prin propriile proceduri interne. De asemenea, trebuie să actualizeze constant aceste politici, prin raportare la noile procese de prelucrare.

- o Autoritatea de supraveghere daneză (Datatilsynet) a dispus o amendă în cuantum de 160.000 de euro pentru operatorul Taxa 4x35, motivul fiind nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania de taxi nu a respectat principiul minimizării datelor. Aceasta a șters datele pasagerilor după 2 ani, dar nu și celelalte informații privitoare la curse (aproximativ 8.873.333 de curse). Astfel, compania a deținut în continuare numerele de telefon ale acelor persoane.



DE REȚINUT! Operatorul este ținut să respecte duratele de retenție stabilite prin acte normative sau după caz, prin propriile proceduri interne.

Estonia

- o Autoritatea de supraveghere estoniană (aepd) a aplicat o singură amendă unei asociații de locuințe, amenda fiind în cuantum de 500 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Asociația a publicat poze ale membrilor fără consimțământul lor.



DE REȚINUT! Interesele legitime ale operatorilor trebuie să fie corelate de activitatea operatorului și de eventualul beneficiu pe care acesta l-ar avea în cadrul unor eventuale activități de promovare. În caz contrar, se impune colectarea consimțământului persoanelor vizate de astfel de prelucrări.

Finlanda

Autoritatea de supraveghere finlandeză (aepd) a aplicat un număr de 4 amenzi, toate în 2020, pentru nerespectarea cerințelor GDPR, principalul motiv sancționat constând în nerespectarea principiilor de prelucrare.

- o Autoritatea de supraveghere finlandeză a dispus sancționarea operatorului Taksi Helsinki cu amendă în cuantum de 72.000 de euro din cauza nerespectării principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Printre altele, compania nu a evaluat riscurile și consecințele prelucrării datelor personale înainte de a instala o cameră de supraveghere ce înregistra audio-video în taxiuri. De asemenea, prelucrarea datelor nu respecta principiul minimizării.



DE REȚINUT! Evaluările de impact sunt esențiale pentru prelucrările de date ce implică riscuri privind drepturile persoanelor vizate și se realizează anterior implementării de noi mijloacele prin intermediul cărora se prelucrează datele.

- o Autoritatea de supraveghere finlandeză a dispus sancționarea operatorului Posti Group Oyj cu amendă în cuantum de 100.000 de euro pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au existat multiple plângeri din partea persoanelor vizate din care a rezultat faptul că acestea au primit mesaje de marketing, deși au solicitat ca datele lor să fie șterse. Investigația a arătat și faptul că informațiile referitoare la protecția datelor oferite de către companie nu erau destul de transparente.



DE REȚINUT! Un alt principiu foarte important, separat de cel al minimizării prelucrării, este cel al transparenței. Operatorul trebuie să

informeze corect și complet persoana vizată cu privire la procesele de prelucrare.

- o Autoritatea de supraveghere finlandeză a sancționat cu amendă în cuantum de 15.000 de euro operatorul Kymen Vesi Oy pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania nu a realizat o evaluare de impact cu privire la datele prelucrate prin intermediul mijloacelor de geolocalizare.



DE REȚINUT! Prelucrarea de date de geolocalizare în materie de relații de muncă are la bază, de regulă, interesele legitime ale angajatorului. Cu toate acestea, operatorul trebuie să realizeze DPIA pentru datele astfel prelucrate, recomandabil înainte de începerea prelucrării de date prin intermediul sistemului GPS.

- o Autoritatea de supraveghere finlandeză a sancționat cu amendă în cuantum de 12.500 o companie, motivul fiind insuficientul temei pentru prelucrarea datelor angajaților.

Franța

Autoritatea de supraveghere franceză (CNIL) a aplicat un număr de 5 amenzi, toate în 2019, pentru nerespectarea cerințelor GDPR, principalul motiv sancționat constând în insuficiența măsurilor tehnice și organizatorice.

- o Autoritatea de supraveghere franceză (CNIL) a sancționat cu amendă în cuantum de 500.000 de euro operatorul Futura Internationale pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a fost sancționată după ce mai mulți reclamanți au fost contactați telefonic, deși au precizat expres faptul că nu vor să primească apeluri. Investigația a dezvăluit, printre altele, că erau stocate excesiv informații despre clienți și starea lor de sănătate și că respectiva companie nu a informat persoanele despre procesarea datelor personale sau despre înregistrarea conversațiilor telefonice.



DE REȚINUT! Operatorul trebuie să analizeze orice solicitare privind exercitarea drepturilor persoanelor vizate și să îi dea curs, în măsura în care aceasta este justificată.

o Autoritatea de supraveghere franceză (CNIL) a sancționat cu amendă în cuantum de 180.000 de euro operatorul ACTIVE ASSURANCES, pe motivul măsurilor tehnice și organizatorice de protecție a informației insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un număr mare de conturi ale clienților, documente ale acestora (inclusiv copii ale permiselor de conducere, înregistrările autovehiculelor și alte documente) și date au fost ușor accesibile online. Printre altele, autoritatea de supraveghere a criticat management-ul parolelor, deoarece era posibil accesul neautorizat fără orice autentificare.



DE REȚINUT! Operatorul trebuie să implementeze o serie de măsuri tehnice menite să asigure securitatea informațiilor prin raportare la specificul activității desfășurate. Acestea includ, dar nu se limitează la autentificarea unică a membrilor personalului, securizarea serverelor, protejarea rețelei de internet etc.

o Autoritatea de supraveghere franceză (CNIL) a sancționat cu amendă în cuantum de 20.000 de euro operatorul UNIONTRAD COMPANY pentru insuficiența temeiului de prelucrare a datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: În perioada 2013-2017, autoritatea de supraveghere a primit numeroase plângeri de la angajații companiei care erau filmați la locul de muncă. Au fost semnalate companiei de două ori regulile ce trebuie urmate atunci când se instalează camere la locul de muncă, mai exact faptul că angajații nu ar trebui filmați constant și că trebuie furnizate informații referitoare la prelucrare. Din cauza faptului că la sfârșitul termenului fixat inițial nu au fost adoptate măsuri satisfăcătoare, autoritatea a derulat o nouă investigație în 2018, confirmându-se faptul că angajatorul încălca în continuare legile pentru protecția datelor.



DE REȚINUT! Companiile trebuie să evite instalarea de mijloace de supraveghere video în birouri, toalete, vestiare sau orice alte locuri în care, în mod rezonabil, angajatul are nevoie de intimitate. Instalarea de camere video în birouri a fost sancționată și la nivelul României.

o Autoritatea de supraveghere franceză (CNIL) a dispus aplicarea unei amenzi în cazul unei companii de real estate, SERGIC, în cuantum de 400.000 de euro, pentru insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost bazată pe două aspecte: lipsa măsurilor de securitate de bază și stocarea excesivă a datelor. Pentru prima parte, documente ale utilizatorilor postate de către posibili chiriași (inclusiv cărți de identitate, carduri de sănătate, certificate, sentințe de divorț) au fost ușor accesibile online, fără a fi necesară o procedură de autentificare. Deși problema era cunoscută de companie încă din martie 2018, aceasta a fost soluționată complet abia în septembrie 2018. În plus, compania stoca documentele primite pentru mai mult timp decât era necesar.



DE REȚINUT! Operatorul trebuie să acționeze imediat în cazul unei breșe de securitate, pasivitatea putând atrage o sancțiune mai aspră, mai ales în contextul în care obiectul breșei de securitate este reprezentat de date sensibile.

o Autoritatea de supraveghere franceză (CNIL) a dispus sancționarea operatorului Google Inc. cu amendă în cuantum de 50.000.000 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a venit în urma unor plângeri formulate pe 25 și 28 mai 2018, imediat după ce GDPR a devenit aplicabil și vizau crearea unui cont Google în cadrul configurării unui telefon mobil cu sistem de operare Android. Sancțiunea a fost aplicată pentru lipsa transparenței, informații insuficiente și lipsa unui temei legal. Consimțământul obținut nu a fost dat expres și clar.



DE REȚINUT! Consimțământul oferit pentru prelucrarea datelor trebuie să fie expres, nu condiționat sau inserat în conținutul unor clauze ce nu pot fi negociate.

Germania

Autoritățile de supraveghere germane au aplicat un număr de 24 amenzi pentru nerespectarea cerințelor GDPR, principalele motive sancționate constând în insuficiența măsurilor tehnice și organizatorice, insuficiența temeiurilor de prelucrare și nerespectarea principiilor generale ale prelucrărilor de date.

o În anul 2020 a fost aplicată o singură sancțiune, de către Autoritatea pentru Protecția Datelor din Baden-Wuerttemberg. Operatorul Allgemeine

Ortskrankenkasse, o societate de asigurări de sănătate, a fost amendată cu 1.240.000 de euro, pe motivul măsurilor tehnice și organizatorice insuficiente pentru securitatea informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: În perioada 2015-2019, societatea de asigurări a organizat competiții cu diferite ocazii și a colectat datele personale ale participanților, inclusiv detalii contractuale și afilierea asigurării de sănătate. Societatea dorea, de asemenea, să folosească datele în scopuri de promovare cu consimțământul participanților. Se dorea ca prin măsuri tehnice și organizaționale, inclusiv ghiduri interne și traininguri pentru protecția datelor, să fie folosite doar datele acelor participanți care și-au dat consimțământul. Totuși, măsurile nu au îndeplinit cerințele legale și, drept rezultat, datele personale a peste 500 de participanți au fost utilizate în scopuri de promovare fără consimțământul lor.



DE REȚINUT! Este foarte important ca planul de conformare să nu fie unul formal, iar măsurile stabilite să fie implementate în mod eficient. Un element ce ar putea constitui o circumstanță atenuantă pentru operator ar fi stoparea de îndată a prelucrărilor și efectuarea urgentă a unor investigații interne care să indice sursa care a condus la incidentul de securitate, urmată de implementarea unor măsuri de remediere.

Pe parcursul anului 2019 au fost aplicate 19 amenzi pentru nerespectarea cerințelor GDPR:

- o Comisarul Federal pentru Protecția Datelor și Libertatea Informației a sancționat un furnizor de service telecom cu suma de 9.550.000 de euro, motivul fiind insuficiența măsurilor tehnice și organizatorice de protecție a informațiilor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un apelant putea obține informații extensive despre datele personale ale clienților de la departamentul de relații cu clienții al companiei, doar prin introducerea numelui clientului și datei de naștere.



DE REȚINUT! Companiile trebuie să implementeze măsuri de securitate adecvate și care să nu permită cu ușurință divulgarea datelor privind persoana vizată. Operatorii care trebuie să pună la dispoziția persoanelor vizate informații sensibile precum rezultate ale unor analize, diferite teste, verificări etc. pot opta pentru furnizarea datelor pe bază de user și parole de acces.

◦ Comisarul Federal pentru Protecția Datelor și Libertatea Informației a sancționat operatorul Rapidata GmbH cu amendă în cuantum de 10.000 de euro pentru lipsa desemnării unui responsabil cu protecția datelor (DPO).



DE REȚINUT! GDPR nu prevede expres cazurile în care este necesară desemnarea DPO-ului, fiind necesar ca operatorul să constate dacă realizează prelucrări sistematice sau pe scară largă. Cu toate acestea, acolo unde volumul de date este foarte mare (magazine online, unități de cazare, școli, grădinițe, spitale/clinici etc.), este recomandat ca numirea DPO-ului să fie o prioritate.

◦ Autoritatea pentru Protecția Datelor din Rheinland-Pfalz a sancționat cu amendă în cuantum de 105.000 un spital din cauza insuficienței măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda vine ca urmare a numeroase încălcări ale GDPR, în legătură cu o serie de erori cu privire la pacienți, din care a rezultat facturarea greșită, fapt ce a relevat deficitele tehnice și organizaționale în managementul pacienților.



DE REȚINUT! Când volumul de date este foarte mare, iar personalul se modifică foarte des, compania ar trebui să aibă în vedere sesiuni de instruire organizate periodic și de inițiere, pentru fiecare nou angajat care intră în contact cu date, mai ales dacă avem în vedere date prelucrate la nivelul unui spital sau al unei clinici, al unei bănci, școli etc.

◦ Autoritatea pentru Protecția Datelor din Berlin a amendat Deutsche Wohnen SE cu 14.500.000 de euro, motivul fiind nerespectarea principiilor generale ale prelucrării datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a utilizat un sistem de arhivare pentru stocarea datelor personale ale chiriașilor ce nu oferea posibilitatea eliminării datelor ce nu mai erau necesare. Datele erau stocate fără a verifica dacă stocarea era permisă sau necesară. Astfel, a fost posibilă accesarea datelor personale ale respectivilor chiriași care au fost stocate timp de mai mulți ani, fără ca datele să mai îndeplinească scopurile pentru care au fost colectate inițial. Erau implicate și date personale importante privind aspecte financiare, precum declarații de salariu, extrase din contracte de angajare și pregătire sau date despre asigurări.



DE REȚINUT! Operatorul răspunde de conformitatea sistemelor informatice pe care le utilizează în activitate. Un argument potrivit căruia sistemul nu permite gestionarea corectă a datelor personale nu ar putea fi reținut în cadrul unei investigații.

o Autoritatea pentru Protecția Datelor din Baden-Wuerttemberg a sancționat o companie din sectorul alimentar cu amendă în cuantum de 100.000 de euro pentru insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a creat un portal pentru solicitanți pe site-ul său, unde părțile interesate puteau să trimită online documentele pentru aplicația lor, dar compania nu a asigurat transmiterea criptată a datelor și nici nu le-a stocat în mod criptat sau protejat de parole. De asemenea, datele applicantului erau conectate la Google, astfel încât oricine căuta numele persoanei respective pe Google putea să găsească documentele respective, fără a exista restricții de acces.



DE REȚINUT! Odată pus la dispoziție publicului un larg un sistem colector de date, operatorul trebuie să se asigure că implementează măsuri de securitate adecvate.

o Autoritatea pentru Protecția Datelor din Berlin a sancționat operatorul Delivery Hero cu o amendă în cuantum de 195.407 euro pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Potrivit investigației, compania nu a șters conturile foștilor clienți în 10 cazuri diferite, deși persoanele respective nu au fost active pe platforma de servicii a companiei timp de mai mulți ani (din 2008 într-un caz). În plus, opt foști clienți au formulat plângeri referitoare la e-mailuri de marketing nesolicitate. O persoană care a refuzat expres utilizarea datelor sale în scopuri de promovare a primit 15 e-mailuri de la furnizorul de servicii. În alte 5 cazuri, compania nu a oferit persoanelor vizate informațiile solicitate sau a făcut-o abia după intervenția autorității din Berlin.



DE REȚINUT! Procedurile interne privind retenția datelor ar trebui să prevadă o durată maximă pentru care pot fi stocate datele persoanelor care și-au creat cont pe o anumită platformă. Este adevărat că majoritatea operatorilor doresc să țină conturile active cât mai mult

posibil, pentru a facilita accesul în cazul unei eventuale reveniri a clientului, însă o absență justificată din platformă nu justifică prelucrarea în continuare a datelor respective.

- o Autoritatea pentru Protecția Datelor din Nordrhein-Westfalen a dispus o amendă de 200 de euro pentru o persoană fizică, titulară a unui canal de Youtube, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Persoana respectivă a folosit o cameră de supraveghere auto pentru înregistra traficul de pe un drum public și ulterior a postat înregistrările pe Youtube.



DE REȚINUT! Inclusiv persoanele fizice trebuie să demonstreze responsabilitate în materie de protecție a datelor. În cazul în care se publică filmări personale, persoana în cauză poate elimina anumite secțiuni/secvențe cu ajutorul cărora pot fi identificate persoanele vizate.

- o Autoritatea pentru Protecția Datelor din Baden-Wuerttemberg a sancționat un ofițer de poliție cu amendă în cuantum de 1.400 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Polițistul, folosindu-se de funcția sa, a intrat în posesia mai multor date personale pe care le-a folosit în scopuri personale, fără consimțământul acesteia. În acest fel, polițistul a procesat date personale în depășirea autorității cu care era învestit.



DE REȚINUT! Personalul care intră în contact cu datele personale trebuie să fie instruit, astfel încât să înțeleagă riscurile aferente prelucrării datelor în alte scopuri decât cele avute în vedere la momentul colectării, inclusiv în interes personal. Angajatorul poate introduce sancțiuni în regulamentul intern pentru a da eficiență acestor reguli interne.

- o Autoritatea pentru Protecția Datelor din Baden-Wuerttemberg a aplicat o sancțiune de 80.000 de euro unei companii din sectorul financiar pentru insuficiența măsurilor tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania nu a reușit să ia măsurile necesare pentru a asigura integritatea și confidențialitatea informației atunci când a divulgat documente ce conțineau datele personale a doi clienți. Astfel, fără anonimizare anterioară, documentele au fost disponibile în locația de reciclare a hârtiei, unde au fost găsite de o persoană neautorizată.



DE REȚINUT! Anterior predării documentelor confidențiale pentru care a expirat perioada de retenție sau a oricăror alte tipuri de documente ce conțin date personale, se recomandă ca acestea să fie introduse într-un shredder pentru a preîntâmpina orice incident de securitate derivat din accesarea neautorizată a datelor.

- o Autoritatea pentru Protecția Datelor din Berlin a aplicat o amendă în cuantum de 50.000 de euro operatorului N26, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată pentru prelucrarea unor date personale ale foștilor clienți fără acordul lor. Banca a recunoscut faptul că a păstrat datele pentru a întocmi o listă neagră, un document care să fie o atenționare de a nu deschide un nou cont acelor persoane.



DE REȚINUT! O astfel de listă neagră păstrată fără a exista o obligație legală poate aduce atingeri grave drepturilor persoanelor vizate. Anterior implementării unui astfel de proiect, compania ar trebui să analizeze riscurile asociate acestei prelucrări și să întocmească o evaluare de impact.

- o Autoritatea din Sachsen-Anhalt pentru Protecția Datelor a aplicat o sancțiune cu amendă în cuantum de 2.500 de euro pentru insuficiența temeiului de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost acordată, deoarece persoana respectivă a trimis mai multe e-mailuri în perioada iulie-septembrie 2018, utilizând adresele personale de e-mail vizibile pentru toți destinatarii, fiecare putând să vadă numeroși alți destinatari. Persoana a fost acuzată de 10 încălcări de la jumătatea până la finalul lunii iulie. Între 131 și 135 de adrese de e-mail personale puteau fi identificate.



DE REȚINUT! Inclusiv persoanele fizice care prelucrează date trebuie să demonstreze responsabilitate și să preîntâmpine incidente ce ar putea deriva din prelucrările de date.

- o Autoritatea pentru Protecția Datelor din Baden-Württemberg a dispus sancționarea cu amendă în cuantum de 80.000 de euro unui operator pentru insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Într-o publicație digitală, date despre sănătate au fost publicate accidental din cauza mecanismelor interne de control inadecvate.



DE REȚINUT! Compania trebuie să acorde o atenție sporită sistemelor informatice pe care le utilizează în activitate pentru a preveni orice incident de securitate.

- o Autoritatea pentru Protecția Datelor din Mecklenburg-Vorpommern a sancționat cu amendă un polițist, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Polițistul a folosit datele personale ale unui martor pentru a-l contacta personal.



DE REȚINUT! Personalul care intră în contact cu datele personale trebuie să fie instruit astfel încât să înțeleagă riscurile aferente prelucrării datelor în alte scopuri decât cele avute în vedere la momentul colectării, inclusiv în interes personal. Angajatorul poate introduce sancțiuni în regulamentul intern pentru a da eficiență acestor reguli interne.

- o Autoritatea pentru Protecția Datelor din Niedersachsen a aplicat o amendă în cuantum de 294.000 de euro pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a fost sancționată pentru stocarea de lungă durată fără a fi necesar a documentelor de personal, dar și pentru stocarea excesivă de date în cadrul procesului de selecție a personalului, în acest context fiind cerute și date despre sănătate.



DE REȚINUT! În cadrul proceselor de recrutare, angajatorul va respecta principiul minimizării și se va limita strict la datele necesare pentru recrutare. De asemenea, dacă nu intenționează să utilizeze datele colectate în cadrul unor viitoare procese de prelucrare informând persoana vizată în acest sens, va șterge informațiile după interviu sau după caz, după finalizarea procesului de recrutare.

- o Autoritatea pentru Protecția Datelor din Hamburg a sancționat Facebook Germany GmbH cu amendă în cuantum de 51.000 de euro, motivul fiind lipsa desemnării unui DPO.

Situația de fapt ce a stat la baza aplicării sancțiunii: Deși Facebook Irlanda a numit un DPO pentru toate companiile din grup situate în Europa, numirea nu a fost notificată autorității din Hamburg.



DE REȚINUT! Deși poate fi acceptată noțiunea de DPO pentru un grup de companii, trebuie avută în vedere procedura notificării acestuia la autoritățile de supraveghere competente.

- o Autoritatea pentru Protecția Datelor din Hamburg a sancționat Hamburger Verkehrsverbund GmbH (HVV GmbH) cu amendă în cuantum de 20.000 de euro, motivul fiind neîndeplinirea obligației de notificare privind încălcarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Pe data de 6 iulie 2018, compania a fost informată de către un client despre o breșă de securitate pe site-ul său cauzată de un update în data de 5 februarie 2018. Clienții se autentificau pe serviciul online de relații cu clienții ce aveau card HVV și conturile erau conectate cu cel puțin o relație contractuală activă în sistem, iar schimbând URL-ul, se puteau afișa datele altor clienți posesori ai unui card HVV. Încălcarea nu a fost raportată în timp util autorității de supraveghere.



DE REȚINUT! De cele mai multe ori, companiile nu notifică astfel de breșe de securitate, considerând că incidentul nu este semnificativ. Cu toate acestea, pentru a preîntâmpina orice eventuală problemă legată de notificarea breșelor de securitate, se recomandă implementarea unei proceduri eficiente de analiză a incidentelor de securitate, indiferent de gravitatea lor. Esențială în acest sens este și instruirea angajaților, care trebuie să știe să identifice incidentele de securitate și ulterior să declare de îndată existența lor persoanelor responsabile și DPO-ului, care trebuie implicat în astfel de verificări interne.

- o Autoritatea pentru Protecția Datelor din Hamburg a sancționat Hamburger Volksbank eG pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a trimis unui client un newsletter deși clientul a obiectat anterior la trimiterea mesajelor de promovare.



DE REȚINUT! Companiile care desfășoară activități de marketing prin transmiterea de newsletter trebuie să se asigure de faptul că au

un temei legal în baza căruia pot comunica cu persoana vizată. Acest temei este, ca regulă generală, consimțământul însă putem întâlni și situații în care transmiterea de newsletter are la bază interesele legitime ale companiei.

- o Autoritatea pentru Protecția Datelor din Saarland a sancționat un restaurant cu amendă în cuantum de 2.000 de euro pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost utilizate camere de supraveghere video ce monitorizau și zone pentru clienți din restaurant, încălcându-se astfel principiul minimizării datelor.



DE REȚINUT! Mijloacele de supraveghere video nu trebuie privite ca fiind interzise prin raportare la practica autorităților de supraveghere. Deși multe sancțiuni aplicate la nivel european vizează acest aspect, trebuie observat faptul că simpla existență a unor astfel de mijloace nu ridică probleme. Cu toate acestea, compania trebuie să evite instalarea camerelor video în locul în care sunt situate mesele (zonele de clienți), dacă ne raportăm la un restaurant, birourile, dacă ne raportăm la relațiile de muncă, vestiarele dacă ne raportăm la o sală de fitness etc.

- o Autoritatea pentru Protecția Datelor din Brandenburg a sancționat o companie cu suma de 50.000 de euro pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un operator de date a angajat o companie externă să îndeplinească obligațiile privind accesul la date, dar aceasta a realizat corespondența cu persoanele vizate în nume propriu și în limba engleză, nefiind clar persoanelor vizate cine era responsabil pentru prelucrarea de date. Astfel, a fost încălcat principiul transparenței. De asemenea, autoritatea de supraveghere a observat faptul că nu exista un acord de prelucrare între operatorul de date și compania externă.



DE REȚINUT! În cazul în care se optează pentru externalizarea anumitor servicii, compania trebuie să se asigure că furnizorul comunică cu persoanele vizate ale căror date sunt deținute de companie în numele și pe seama companiei, în caz contrar putându-se ridica problema nerespectării principiului transparenței prelucrării. Se recomandă ca astfel de instrucțiuni privind comunicările furnizorului să fie cuprinse într-un acord de prelucrare, care ajută și la demonstrarea legalității

accesului la date pe care îl primește furnizorul de servicii din partea companiei.

Pe parcursul anului 2018 au fost aplicate 5 amenzi pentru nerespectarea cerințelor GDPR:

- o Autoritatea pentru Protecția Datelor din Hamburg a sancționat compania Kolibri Image Regina und Dirk Maass GbR cu amendă în cuantum de 5.000 de euro pentru lipsa unui acord de prelucrare.



DE REȚINUT! Deși nu este necesar în orice relație contractuală, acordul privind prelucrarea datelor trebuie privit ca un instrument eficient ce demonstrează conformitatea operatorului. Acordurile de prelucrare nu au o formă standard, putând fi cuprinse atât în contracte ori în acte adiționale la contracte dar și încheiate separat.

- o Autoritatea pentru Protecția Datelor din Baden-Wuerttemberg a sancționat compania Knuddels.de cu amendă în cuantum de 20.000 de euro pentru lipsa unor măsuri tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: În urma unui atac informatic, datele a aproximativ 330.000 de utilizatori, inclusiv parole și adrese de e-mail, au fost dezvăluite.



DE REȚINUT! Companiile trebuie să depună toate diligențele, astfel încât să preîntâmpine orice eventuale incidente de securitate (furt, pierdere, atac etc.).

- o Autoritatea pentru Protecția Datelor din Hamburg a aplicat o sancțiune cu amendă în cuantum de 20.000 de euro pentru neîndeplinirea obligației de notificare privind încălcarea securității datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amendă a fost aplicată pentru notificarea târzie a încălcării securității datelor și lipsa notificării persoanelor vizate.



DE REȚINUT! Atunci când incidentul de securitate este susceptibil să aducă atingeri grave drepturilor persoanelor vizate, pe lângă notificarea autorității compania trebuie să ia în calcul și notificarea persoanelor vizate.

Autoritățile germane au aplicat și alte sancțiuni cu privire la care nu există detalii.

Grecia

Autoritatea de supraveghere din Grecia a aplicat un număr total de 9 amenzi, principalele aspecte sancționate constând în nerespectarea drepturilor persoanelor vizate și nerespectarea principiilor generale de prelucrare.

În anul 2020 au fost aplicate 4 sancțiuni pentru nerespectarea GDPR:

- o Autoritatea Elenă pentru Protecția Datelor (HDPa) a aplicat o sancțiune în cuantum de 5.000 de euro operatorului New York College S.A. pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Operatorul a contactat reclamantul direct, prin telefon, în legătură cu un program educațional și nu a prelucrat datele într-o manieră transparentă.



DE REȚINUT! Atunci când operatorul optează pentru contactarea telefonică a persoanei vizate ar trebui să se asigure că există această așteptare din partea persoanei vizate (de exemplu, în funcție de canalul pentru care s-a optat în vederea comunicărilor).

- o Autoritatea Elenă pentru Protecția Datelor (HDPa) a aplicat o sancțiune în cuantum de 8.000 de euro operatorului Speech and Special Education Centre – Mihou Dimitra pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Reclamantul a solicitat acces la datele copilului său și la informații referitoare la taxe. Solicitarea i-a fost respinsă de către operatorul de date. În plus, acesta a încălcat un ordin al autorității de supraveghere privind accesul la date. Amenda a constat în 3.000 de euro pentru lipsa garantării accesului la datele personale și 5.000 de euro pentru încălcarea ordinului respectiv.



DE REȚINUT! Operatorul trebuie să furnizeze acces la datele persoanei vizate atunci când aceasta își exercită dreptul de acces la datele sale. Răspunsul pentru astfel de cereri nu trebuie transmis mai târziu de o lună de la data primirii solicitării.

- o Autoritatea Elenă pentru Protecția Datelor (HDPa) a aplicat o amendă în cuantum de 5.000 de euro societății Public Power Corporation S.A. pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Decizia a clarificat faptul că persoanele vizate au drept de acces la procesarea datelor

personale și că trebuie să li se pună la dispoziție o copie a datelor procesate, nefiind necesare motive pentru astfel de solicitări.



DE REȚINUT! În cazul în care persoana vizată își exercită dreptul de acces, compania este obligată să îi dea curs și să ofere datele solicitate, fără a solicita justificări din partea persoanei vizate. O eventuală ștergere a datelor în condițiile în care a fost depusă o cerere de acces poate fi sancționată de către autoritate.

- o Autoritatea Elenă pentru Protecția Datelor (HDPa) a aplicat o sancțiune în cuantum de 15.000 de euro societății Allseas Marine S.A. pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a venit ca urmare a prelucrării datelor angajaților prin supravegherea video la locul de muncă, instalarea sistemului fiind nelegală. De asemenea, s-a constatat că informarea salariaților cu privire la aceste mijloace nu este completă.



DE REȚINUT! Angajatorul va evita instalarea de mijloace de supraveghere video în cadrul birourilor, considerându-se de către autoritățile de supraveghere că acestea sunt de natură a aduce atingere dreptului la viață privată a persoanelor vizate. De asemenea, angajatorul va avea în vedere să informeze persoanele vizate cu privire la existența camerelor prin intermediul pictogramelor specifice și va afișa note de informare cu detaliile prelucrării.

În anul 2019 au fost aplicate 5 sancțiuni pentru nerespectarea GDPR:

- o Autoritatea Elenă pentru Protecția Datelor (HDPa) a aplicat o amendă în cuantum de 150.000 de euro operatorului Aegean Marine Petroleum Network Inc. pentru insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Companiile care nu făceau parte din Aegean Marine Petroleum Group au avut acces la servere ce conțineau date cu caracter personal și au copiat conținutul acestora, deoarece nu au fost luate măsuri de siguranță suficiente. De asemenea, persoanele vizate nu au fost informate privind procesarea datelor stocate pe server.



DE REȚINUT! Compania trebuie să implementeze măsuri de securitate care să prevină accesul nepermis și posibilitatea de a copia/transferea date de către persoane neautorizate.

o Autoritatea Elenă pentru Protecția Datelor (HDPa) a dispus sancționarea operatorului Wind Hellas Telecommunications cu suma de 20.000 de euro pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Printre altele, compania a ignorat obiecțiile ridicate de către persoanele afectate în ceea ce privește apelurile de marketing.



DE REȚINUT! Compania trebuie să poate demonstra legalitatea comunicărilor realizate în scopuri de marketing. În acest sens se va face dovada consimțământului ori după caz, a existenței intereselor legitime ce au la bază relația relevantă dintre companie și persoana vizată.

o Autoritatea Elenă pentru Protecția Datelor (HDPa) a aplicat o amendă în cuantum de 200.000 de euro unui furnizor de servicii de telecomunicații pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Mai mulți clienți au fost sunați în scop de marketing, deși au optat să nu fie contactați în acest sens, dar decizia acestora nu a putut fi respectată din cauza unor erori tehnice.



DE REȚINUT! Compania trebuie să poate demonstra legalitatea comunicărilor realizate în scopuri de marketing.

o Autoritatea Elenă pentru Protecția Datelor (HDPa) a aplicat o sancțiune cu amendă în cuantum de 200.000 de euro unui furnizor de servicii de telecomunicații pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Din cauza unor măsuri tehnice inadecvate, datele personale a 8.000 de clienți nu au fost șterse la cerere.



DE REȚINUT! Insuficiența măsurilor tehnice este frecvent sancționată de către autoritățile de supraveghere europene. Eventualele

argumente bazate pe erori tehnice ale sistemelor nu sunt de natură a exonera compania de responsabilitate.

- o Autoritatea Elenă pentru Protecția Datelor (HDPa) a dispus sancționarea PWC Business Solutions cu amendă în cuantum de 150.000 de euro, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Prelucrarea datelor cu caracter personal ale angajaților s-a realizat pe bază de consimțământ. Autoritatea de supraveghere a descoperit faptul că în acest caz consimțământul ce constituia baza legală era inadecvat, prelucrarea fiind realizată pentru operațiuni direct legate de executarea contractelor de muncă. Așadar, compania a lăsat angajaților falsa impresie că prelucra datele personale pe baza legală a consimțământului, în timp ce, în realitate, baza legală era una diferită. Astfel, a fost încălcat principiul transparenței.



DE REȚINUT! În practică, întâlnim frecvent formularea de consimțământ pentru relații de muncă, deși temeiul legal al prelucrării este, de cele mai multe ori, obligația legală a angajatorului. Companiile trebuie să analizeze temeiurile corecte și să le aplice, existând riscul încălcării principiului transparenței.

Irlanda

Autoritatea pentru Protecția Datelor din Irlanda a aplicat doar două amenzi pentru nerespectarea GDPR, ambele pe parcursul anului 2020.

- o Autoritatea pentru Protecția Datelor din Irlanda a sancționat operatorul Tusla Child and Family Agency cu o amendă în cuantum de 40.000 de euro din cauza neîndeplinirii obligației de notificare privind încălcarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Organizația a transmis o scrisoare cu acuzații de abuz unei terțe persoane, care a postat-o ulterior pe rețelele de socializare.



DE REȚINUT! Operatorul trebuie să implementeze măsuri menite să prevină astfel de incidente. Ca o primă precauție, se poate avea în vedere marcarea documentelor cu mențiunea „confidențial” sau „strict confidențial”.

- o Autoritatea pentru Protecția Datelor din Irlanda a dispus sancționarea operatorului cu amendă în cuantum de 75.000 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a dezvăluit în mod eronat date personale, inclusiv informații despre copii, unor persoane neautorizate. Într-un anumit caz, datele de contact și de localizare ale unei mame cu un copil au fost dezvăluite unui presupus infractor și, în alte două cazuri, date despre copii în asistență maternală au fost dezvăluite rudelor biologice, inclusiv într-un caz în care tatăl era în închisoare.



DE REȚINUT! Companiile trebuie să implementeze măsuri de securitate adecvate și care să nu permită cu ușurință divulgarea datelor privind persoana vizată. Operatorii care trebuie să pună la dispoziția persoanelor vizate informații sensibile pot opta pentru furnizarea datelor pe bază de user și parole de acces.

Italia

Autoritatea de supraveghere italiană a dispus un număr de 16 sancțiuni, principalul aspect sancționat constând în insuficiența temeiului legal de prelucrare.

În anul 2020 au fost înregistrate 13 sancțiuni pentru nerespectarea GDPR:

- o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat compania Merlini S.R.L. cu amendă în cuantum de 200.000 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea a desfășurat activități de telemarketing în numele Wind tre S.p.A. prin intermediul unui furnizor terț, în calitate de operator de date, fără un temei juridic suficient pentru prelucrarea datelor și fără acord de prelucrare acoperitor cu furnizorul terț.



DE REȚINUT! Deși nu este necesar în orice relație contractuală, acordul privind prelucrarea datelor trebuie privit ca un instrument eficient ce demonstrează conformitatea operatorului. Acordurile de prelucrare nu au o formă standard, putând fi cuprinse atât în contracte ori în acte adiționale la contracte dar și încheiate separat.

- o Autoritatea pentru Protecția Datelor din Italia (Garante) a dispus sancționarea companiei Wind Tre S.p.A. cu amendă în cuantum de 16.700.000 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Sute de persoane vizate au pretins că au primit comunicări nesolicitate, trimise fără consimțământul lor prealabil prin SMS, e-mail, apeluri telefonice și apeluri automate. Persoanele vizate nu au putut să își exercite dreptul de a-și retrage consimțământul și de a se opune prelucrării în scopuri de marketing direct, deoarece informațiile cuprinse în politica de protecție a datelor erau incomplete în ceea ce privește datele de contact. În plus, autoritatea pentru protecția datelor a declarat că datele persoanelor vizate au fost publicate pe listele telefonice publice, în pofida obiecției acestora. De asemenea, au fost create mai multe aplicații distribuite de către companie, astfel încât utilizatorul a trebuit să își dea consimțământul pentru diferite activități de prelucrare de fiecare dată când a accesat aceste aplicații, cu posibilitatea de a-și retrage consimțământul acordat numai după 24 de ore.



DE REȚINUT! Retragera consimțământului pentru prelucrare trebuie să poată opera oricând, persoana vizată neputând fi condiționată în a aștepta un anumit interval de timp pentru a putea dispune de acest drept.

o Autoritatea pentru Protecția Datelor din Italia (Garante) a aplicat o amendă în cuantum de 800.000 de euro companiei Iliad Italia S.p.A. pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda vizează încălcările normelor privind protecția datelor referitoare la prelucrarea datelor clienților pentru activarea cardurilor SIM și la modul în care au fost înregistrate datele privind plățile. În plus, autoritatea pentru protecția datelor a declarat că societatea a încălcat principiile legalității, corectitudinea și transparența, precum și integritatea și confidențialitatea în ceea ce privește prelucrarea datelor cu caracter personal în scopuri de marketing direct și stocarea datelor cu caracter personal ale clienților în zona sa de internet.



DE REȚINUT! Există spații în care datele persoanele ale clienților care vizitează o anumită incintă pot fi stocate fără ca aceștia să fie de acord cu utilizarea unei rețele de internet. Colectarea datelor se realizează involuntar prin intermediul telefoanelor/tabletelor/device-uri similare ce se conectează automat la rețeaua Wi-Fi. Deși în astfel de situații se poate pune problema intereselor legitime ale operatorului,

trebuie analizate așteptările persoanei vizate de a-i fi colectate datele într-o astfel de manieră. În astfel de cazuri, simpla afișare a unor note de informare nu este de natură să îndeplinească obligația de informare ce îi revine operatorului deoarece atenția persoanei nu este concentrată pe identificarea acestor informații.

- o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat operatorul Liceo Artistico Statale di Napoli cu amendă în cuantum de 4.000 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Liceul a publicat în mod nelegal date medicale și alte informații a peste 2.000 de persoane în clasamentul profesorilor publicat pe site, încălcându-se astfel principiul legalității, dreptății, transparenței și minimizării datelor.



DE REȚINUT! Operatorul, fie că face parte din sectorul public, fie că face parte din sectorul privat, trebuie să identifice temeiul de prelucrare de care dispune pentru prelucrare și dacă acesta este acoperitor pentru toate procesele de prelucrare avute în vedere de operator.

- o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat operatorul San Giorgio Jonico cu amendă în cuantum de 3.000 de euro, motivat de insuficiența temeiului pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost publicate pe un site datele cu caracter personal ale unui cetățean și nu au fost îndeplinite cererile de ștergere a datelor.



DE REȚINUT! Operatorul va da curs solicitărilor persoanelor vizate privind exercitarea drepturilor persoanelor vizate, putând oferi un răspuns negativ doar în cazurile prevăzute de GDPR.

- o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat Comuna Urago cu amendă în cuantum de 4.000 de euro, motivat de insuficiența temeiului pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Consiliul Local a publicat pe site-ul său informații personale ale unei persoane, inclusiv date medicale.



DE REȚINUT! Operatorul de date, fie că face parte din sectorul public, fie că face parte din sectorul privat, trebuie să fie proactiv și să implementeze măsuri care să preîntâmpine astfel de incidente.

o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat RTI – Reti Televisive Italiane s.p.a. cu o amendă de 20.000 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Postul de televiziune a difuzat un material despre prostituția din Elveția, în care persoanele intervievate nu au fost anonimizate suficient.



DE REȚINUT! Libertatea de exprimare trebuie să fie corelată cu principiile generale și temeiurile prelucrării. Într-un astfel de material, puteau fi blurate sau chiar eliminate secvențe care ajutau la identificarea persoanelor vizate.

o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat Comuna Colledara cu amendă în cuantum de 4.000 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost publicate documente referitoare la o licitație publică pe un site, incluzând și date cu caracter personal.



DE REȚINUT! Operatorul, fie că face parte din sectorul public, fie că face parte din sectorul privat, trebuie să identifice temeiul de prelucrare de care dispune pentru prelucrare și dacă acesta este acoperitor pentru toate procesele de prelucrare avute în vedere de operator.

o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat cu amendă în cuantum de 30.000 de euro operatorul Azienda Ospedaliero Universitaria Integrata di Verona, motivul fiind insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a venit ca urmare a accesării datelor medicale de către persoane neautorizate, oferind posibilitatea unui intern și unui radiolog să obțină acces la datele medicale ale colegilor. Ancheta a arătat faptul că măsurile luate de spital pentru a proteja datele medicale au fost insuficiente pentru asigurarea protecției adecvate a datelor personale, rezultând o procesare nelegală.



DE REȚINUT! Accesarea neautorizată a datelor cu caracter personal poate atrage răspunderea companiei, fiind esențială instruirea angajaților care intră în contact cu datele aparținând operatorului.

o Autoritatea pentru Protecția Datelor din Italia (Garante) a dispus sancționarea operatorului Sapienza Università di Roma cu amendă în cuantum de 30.000 de euro din cauza măsurilor tehnice și organizatorice insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Universitatea a făcut disponibile online datele de identificare a două persoane care au raportat posibile acte ilegale universității, caz în care trebuia ca accesul să fie limitat doar la personalul autorizat în acest sens.



DE REȚINUT! Deși limitarea accesului personalului la date în funcție de atribuțiile angajatului este esențială, multe companii nu tratează cu interes acest aspect, fapt ce permite unor angajați fără drept de acces să vizualizeze date personale.

o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat operatorul de telecomunicații TIM cu amendă în cuantum de 27.800.000 de euro, motivul fiind insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: În perioada ianuarie 2017-2019, autoritatea de supraveghere a primit sute de notificări privind primirea de mesaje comerciale nesolicitate, fără consimțământul persoanelor vizate sau în ciuda obiecțiilor de a primi astfel de mesaje. De asemenea, erau oferite informații incorecte și netransparente în aplicațiile oferite de companie și erau utilizate metode nevalide de obținere a consimțământului. În anumite cazuri, formulare ce solicitau un singur consimțământ erau utilizate în mai multe scopuri, inclusiv marketing. Datele erau păstrate pentru o perioadă mai mare decât era necesar. Printre altele, amenda a fost impusă pentru: lipsa consimțământului pentru activități de marketing, contactarea persoanelor vizate care nu au solicitat acest lucru, consimțământ colectat în mod nevalid în aplicații, lipsa măsurilor de securitate adecvate pentru protejarea datelor personalului, lipsa perioadelor clare de păstrare a datelor.



DE REȚINUT! Compania nu va utiliza datele în scopuri diferite față de cele cunoscute de persoana vizată. De exemplu, societatea nu va transmite newslettere către adresele de e-mail furnizate de clienți în vederea confirmării unei comenzi online.

o Autoritatea pentru Protecția Datelor din Italia (Garante) a dispus aplicarea unei amenzi pentru Comunitatea Francavilla Fontana în cuantum de 10.000 de euro pentru insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost publicate pe site informații privind un litigiu, inclusiv date personale, precum și date medicale privind o persoană.



DE REȚINUT! Operatorul, fie că face parte din sectorul public, fie că face parte din sectorul privat, trebuie să identifice temeiul de prelucrare de care dispune pentru prelucrare și dacă acesta este acoperitor pentru toate procesele de prelucrare avute în vedere de operator.

În anul 2019, au fost înregistrate 3 sancțiuni pentru nerespectarea cerințelor GDPR:

- o Autoritatea pentru Protecția Datelor din Italia (Garante) a sancționat Eni Gas e Luce cu amendă în cuantum de 8.500.000 de euro, motivul fiind insuficiența temeiului de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Printre altele, au fost efectuate apeluri telefonice de promovare fără consimțământul persoanelor contactate sau în ciuda refuzului acestora de a primi astfel de apeluri. De asemenea, exista o lipsă de măsuri tehnice și organizatorice pentru ținerea evidenței informațiilor oferite de utilizatori, datele erau procesate o perioadă mai mare decât perioada de reținere a datelor și datele potențialilor clienți erau colectate de la entități care nu obținuseră consimțământul pentru dezvoltarea acestora.

A doua amendă pentru același operator a fost în cuantum de 3.000.000 de euro, motivul fiind același.

Situația de fapt ce a stat la baza aplicării celei de-a doua sancțiuni: Amendă a fost acordată pentru încălcările rezultate din încheierea contractelor nesolicitate pentru furnizarea energiei electrice și gazului în condițiile economiei de piață. Mai multe persoane au formulat plângeri pentru faptul că au aflat despre încheierea contractelor abia după primirea scrisorilor de încetare a contractelor cu furnizorul anterior sau la prima factură de la noul furnizor. În unele cazuri, s-au raportat informații false în unele contracte, fiind identificate chiar semnături falsificate.



DE REȚINUT! Compania trebuie să poate demonstra legalitatea comunicărilor realizate în scopuri de marketing. În acest sens se va face dovada consimțământului ori după caz, a existenței intereselor legitime ce au la bază relația relevantă dintre companie și persoana vizată.

- o Autoritatea pentru Protecția Datelor din Italia (Garante) a dispus sancționarea partidului politic Movimento 5 Stelle cu amendă în cuantum

de 50.000 de euro din cauza măsurilor tehnice și organizatorice de asigurare a protecției informației insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un număr de site-uri afiliate partidului sunt conduse de către un operator de date prin intermediul unei platforme numite Rousseau. Platforma a suferit o încălcare a securității datelor în vara anului 2017, ceea ce a condus ca autoritatea de supraveghere să solicite implementarea unor măsuri de securitate, pe lângă obligația de a actualiza informațiile despre confidențialitate pentru a asigura o transparență mai mare. Chiar dacă actualizarea a avut loc în timp util, nu au fost implementate anumite măsuri de securitate.



DE REȚINUT! Operatorul trebuie să poată face dovada obținerii consimțământului persoanei vizate sau a oricărui alt temei de prelucrare aplicabil.

Letonia

Autoritatea de supraveghere din Letonia (DSI) a aplicat doar două amenzi pentru nerespectarea GDPR, ambele în anul 2019:

- o Inspectoratul de Stat al Datelor (DSI) a aplicat o amendă în cuantum de 150.000 de euro pentru insuficiența temeiului legal de prelucrare.

- o Inspectoratul de Stat al Datelor (DSI) a dispus sancționarea unui operator de servicii online cu amendă în cuantum de 7.000 de euro pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Magazinul online a încălcat dreptul de a fi uitat când a primit repetate solicitări din partea unei persoane de a-i fi șterse datele personale, mai exact, numărul de telefon la care operatorul trimitea mesaje SMS.



DE REȚINUT! Una dintre cele mai frecvente probleme întâlnite în practică constă în lipsa consimțământului în cadrul prelucrărilor în scopuri de marketing direct. Sigur că operatorul poate lua în calcul și prelucrările de date în scopuri de marketing efectuate în interes legitim, însă doar în acele situații în care există o relație relevantă între operator și persoana vizată (client) și există așteptarea rezonabilă să se comunice astfel de mesaje de către operator. Chiar și în ipoteza în care ar fi justificate

interesele legitime ale operatorului, acesta trebuie să țină cont de obiecțiile, mai ales repetate, ale persoanei vizate.

Lituania

A fost acordată o singură sancțiune de către Autoritatea pentru Protecția Datelor Lituaniană (VDAI) cu amendă în cuantum de 61.500 de euro pentru operatorul UAB MisterTango, motivul fiind îndeplinirea insuficientă a obligației de notificare a încălcării datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: În concret, autoritatea a descoperit faptul că erau procesate mai multe date decât era necesar pentru îndeplinirea scopurilor. În plus, a devenit cunoscut faptul că în perioada 09-10 iulie 2018 datele de plată erau disponibile pe internet din cauza măsurilor inadecvate de protecție. 9.000 de plăți cu 12 bănci din țări diferite au fost implicate. Chiar dacă era necesară o notificare pentru scurgerea de date, aceasta nu a avut loc.



DE REȚINUT! Atunci când incidentul de securitate este susceptibil să aducă atingeri grave drepturilor persoanelor vizate, pe lângă notificarea autorității compania trebuie să ia în calcul și notificarea persoanelor vizate.

Malta

Autoritatea de supraveghere malteză a aplicat o singură sancțiune cu amendă în cuantum de 5.000 de euro pentru nerespectarea GDPR și aceasta a vizat autoritatea funciară, motivul fiind măsurile tehnice și organizatorice insuficiente pentru asigurarea securității informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Drept rezultat al măsurilor de securitate inadecvate privind site-ul autorității funciare, peste 10 Gb de date personale au devenit ușor accesibile publicului prin simpla căutare pe Google. Majoritatea datelor scurse conțineau informații sensibile și corespondențe între mai multe persoane și autoritate.



DE REȚINUT! Operatorul de date, fie că face parte din sectorul public, fie că face parte din sectorul privat, trebuie să fie proactiv și să implementeze măsuri care să preîntâmpine astfel de incidente.

Olanda

Autoritatea de supraveghere din Olanda a aplicat 6 amenzi, principalele aspecte sancționate constând în insuficiența temeiului de prelucrare și a măsurilor tehnice și organizatorice.

În anul 2020 au fost aplicate 3 sancțiuni pentru nerespectarea cerințelor GDPR:

- o Autoritatea de supraveghere olandeză (AP) a sancționat operatorul Bureau Krediet Registratie („BKR”) cu amendă în cuantum de 830.000 de euro pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: BKR a solicitat plata unei taxe atunci când mai multe persoane au solicitat accesul la datele lor personale și au garantat accesul la date doar o dată pe an gratuit prin poștă.



DE REȚINUT! Operatorul poate solicita o taxă rezonabilă atunci când o cerere este vădit nefondată sau excesivă. De asemenea, se poate percepe o taxă dacă se solicită o copie pentru aceleași informații furnizate gratuit anterior. Taxa poate avea în vedere doar costul administrativ al furnizării informațiilor.

- o Autoritatea de supraveghere olandeză (AP) a dispus sancționarea unei organizații cu amendă în cuantum de 725.000 de euro pentru insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Organizația a solicitat angajaților săi să își scaneze amprentele pentru a înregistra prezența. Totuși, decizia autorității arată faptul că nu era vorba de o excepție pentru prelucrarea acestei categorii speciale de date personale, iar compania nu a putut prezenta dovada că angajații și-au dat consimțământul pentru prelucrare.



DE REȚINUT! În cadrul prelucrărilor de date, compania va identifica cele mai puțin intruzive mijloace de prelucrare, mai ales în relațiile de muncă, acolo unde se prezumă că angajatul nu își poate exprima dezacordul cu privire la astfel de măsuri, dat fiind raportul de subordonare.

- o Autoritatea de supraveghere olandeză (AP) a aplicat o amendă în cuantum de 525.000 de euro operatorului Royal Dutch Tennis Association („KNLTB”), motivul fiind insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Asociația a vândut datele personale ale peste 350.000 de membri sponsorilor care au contactat câțiva membri prin e-mail pentru marketing direct. Asociația a vândut date personale, precum nume, gen sau adresă, fără consimțământul persoanelor vizate. Autoritatea a respins argumentul interesului legitim pentru vânzarea datelor și a decis că nu exista o bază legală pentru transferul datelor către sponsori.



DE REȚINUT! Practica vânzării bazelor de date conținând adrese de e-mail a fost foarte răspândită inclusiv pe teritoriul României. Deși acum întâlnim foarte rar în practică astfel de situații, recomandăm operatorilor să fie atenți la orice transfer (chiar cu titlu gratuit) al unor informații atât de sensibile colectate pe bază de consimțământ al persoanei vizate (de exemplu, preferințe). Utilizarea unor astfel de date în alte scopuri decât cele pentru care au fost colectate/de către un alt operator poate atrage răspunderea operatorilor implicați.

În anul 2019 au fost aplicate 3 amenzi pentru nerespectarea cerințelor GDPR:

- o Autoritatea de supraveghere olandeză (AP) a aplicat o amendă în cuantum de 900.000 de euro operatorului UWV, un furnizor de asigurări pentru angajați, motivul fiind măsurile de securitate insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: UWV nu folosea autentificarea cu factori multipli pentru accesarea portalului online al angajatorului. Angajatorii și serviciile de siguranță au putut colecta și dispune de datele medicale ale angajaților.



DE REȚINUT! Operatorul trebuie să implementeze măsuri adecvate care să preîntâmpine accesul neautorizat.

- o Autoritatea de supraveghere olandeză (AP) a dispus sancționarea operatorului Menzis, o companie de asigurări medicale, cu amendă în cuantum de 460.000 de euro pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Angajații responsabili pentru activitățile de marketing au accesat date ale pacienților, încălcând, printre altele, principiul limitării scopului.



DE REȚINUT! Deși limitarea accesului personalului la date în funcție de atribuțiile angajatului este esențială, multe companii nu tratează

cu interes acest aspect, fapt ce permite unor angajați fără drept de acces să vizualizeze date personale.

o Autoritatea de supraveghere olandeză (AP) a sancționat un spital din Haga cu amendă în cuantum de 460.000 de euro pentru insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Spitalul nu are un sistem intern de securitate adecvat pentru registrele pacienților. Investiția a venit ca urmare a faptului că mai mulți angajați ai spitalului au consultat fără a fi necesar dosarul medical al unei persoane cunoscute din Olanda.



DE REȚINUT! Limitarea accesului personalului la date în funcție de treburile tratate prioritar de către operator, fie el din sectorul privat sau public.

Polonia

Autoritatea poloneză de supraveghere a aplicat un număr total de 8 amenzi, principalele aspecte sancționate constând în insuficiența temeiului de prelucrare și în lipsa de cooperare cu autoritatea de supraveghere.

În anul 2020 au fost înregistrate 3 sancțiuni pentru nerespectarea GDPR:

o Oficiul Național Polonez pentru Protecția Datelor cu Caracter Personal (UODO) a aplicat o amendă în cuantum de 3.400 de euro societății East Power Sp. z.o.o., motivul fiind cooperarea insuficientă cu autoritatea de supraveghere.

Situația de fapt ce a stat la baza aplicării sancțiunii: După trei citații transmise către East Power la care aceasta nu a oferit explicații suficiente privind o plângere pentru marketingul direct, autoritatea a descoperit faptul că societatea a obstrucționat desfășurarea procedurii sau, cel puțin, nu a reușit să îndeplinească obligațiile de cooperare.

o Oficiul Național Polonez pentru Protecția Datelor cu Caracter Personal (UODO) a dispus sancționarea companiei Vis Consulting Sp. z.o.o. cu amendă în cuantum de 4.400 de euro, motivul fiind cooperarea insuficientă cu autoritatea de supraveghere.

o Oficiul Național Polonez pentru Protecția Datelor cu Caracter Personal (UODO) a aplicat o amendă în cuantum de 4.600 de euro orașului Gdansk, pentru o Școală din Gdansk, motivul fiind insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Școala a utilizat scannere pentru amprente pentru a autentifica elevii la procesarea plății la cantina școlii. Deși părinții și-au dat consimțământul scris pentru această procesare de date, autoritatea a considerat prelucrarea datelor ca fiind nelegală, deoarece consimțământul nu era dat în mod voluntar.



DE REȚINUT! Operatorul trebuie să poată face dovada îndeplinirii condițiilor unui consimțământ legal.

În anul 2019 au fost aplicate 5 amenzi pentru nerespectarea cerințelor GDPR:

- o Oficiul Național Polonez pentru Protecția Datelor cu Caracter Personal (UODO) a dispus sancționarea primarului din Aleksandrów Kujawski cu suma de 9.380 de euro, motivat de insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Nu a fost încheiat niciun acord de prelucrare a datelor cu compania ale cărei servere conțineau informații ale Buletinului de Informare Publică al Biroului Municipal.

- o Oficiul Național Polonez pentru Protecția Datelor cu Caracter Personal (UODO) a aplicat o amendă în cuantum de 47.000 de euro operatorului ClickQuickNow, motivul fiind nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amendă a fost aplicată pentru obstrucționarea exercitării dreptului la retragerea de la procesare a datelor personale. Compania nu a adoptat măsurile necesare pentru a asigura retragerea simplă și eficientă a consimțământului pentru procesarea datelor personale și exercitarea dreptului de ștergere a datelor personale.



DE REȚINUT! Compania trebuie să ofere posibilitatea persoanei vizate să își retragă consimțământul cel puțin la fel de ușor cum aceasta l-a furnizat.

- o Oficiul Național Polonez pentru Protecția Datelor cu Caracter Personal (UODO) a dispus sancționarea operatorului Morele.net cu amendă în cuantum de 645.000 de euro, motivul fiind insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Măsurile insuficiente au permis accesul neautorizat la datele personale a peste 2.2 milioane de persoane.



DE REȚINUT! Operatorul trebuie să implementeze măsuri adecvate care să preîntâmpine accesul neautorizat.

o Oficiul Național Polonez pentru Protecția Datelor cu Caracter Personal (UODO) a aplicat o amendă în cuantum de 12.950 de euro unei asociații sportive, motivul fiind temeiul legal de prelucrare insuficient.

Situația de fapt ce a stat la baza aplicării sancțiunii: Asociația sportivă a publicat date personale cu privire la judecători cărora le-au fost acordate licențe online, dar nu le-au fost dezvăluite doar numele, ci și adresele exacte și numerele PESEL. S-a creat astfel riscul de utilizare neautorizată a acestor date. Deși asociația a notificat singură propria eroare, faptul că încercările de a remedia problema au fost ineficiente a condus la aplicarea unei sancțiuni.



DE REȚINUT! Operatorul trebuie să poată face dovada obținerii consimțământului persoanei vizate sau a oricărui alt temei de prelucrare aplicabil.

o Oficiul Național Polonez pentru Protecția Datelor cu Caracter Personal (UODO) a aplicat o amendă în cuantum de 220.000 de euro unei companii private ce lucrează cu date din surse disponibile în mod public, motivul fiind îndeplinirea insuficientă a obligațiilor de informare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a vizat activitatea companiei care prelucra datele persoanelor vizate obținute din surse publice, printre care Registrul Electronic Central și le-a procesat în scopuri comerciale. Autoritatea a verificat nerespectarea obligației de informare în legătură cu persoanele fizice care au diverse afaceri, antreprenori cu activitate sau cu activitate suspendată, dar și foști antreprenori. Pentru aceștia a fost îndeplinită obligația de informare, în timp ce, în cazul celorlalte persoane, acest lucru nu s-a întâmplat, din cauza costurilor operaționale ridicate.



DE REȚINUT! Una dintre obligațiile esențiale pe care GDPR le impune companiilor constă în informarea persoanelor vizate.

Portugalia

Autoritatea de supraveghere portugheză a aplicat 4 amenzi pentru nerespectarea cerințelor GDPR, principalul aspect sancționat constând în nerespectarea obligațiilor de informare.

În anul 2019 au fost aplicate 3 amenzi:

- o Autoritatea pentru Protecția Datelor din Portugalia (CNPD) a aplicat două amenzi în cuantum de 2.000 de euro fiecare, motivul fiind îndeplinirea insuficientă a obligațiilor de informare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Nu a fost semnalată folosirea sistemelor CCTV.



DE REȚINUT! Companiile care utilizează sisteme de supraveghere video se vor asigura faptul că acestea sunt semnalizate corespunzător prin intermediul pictogramelor specifice și se vor asigura că durata de retenție este proporțională scopului în care sistemul a fost instalat.

- o Autoritatea pentru Protecția Datelor din Portugalia (CNPD) a dispus sancționarea unui operator cu amendă în cuantum de 20.000 de euro, motivul fiind nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: A fost refuzat dreptul de acces la apelurile înregistrate ale persoanei vizate.



DE REȚINUT! Operatorul trebuie să garanteze accesul persoanei vizate la datele prelucrate cu privire la persoana sa.

- o În anul 2018, Autoritatea pentru Protecția Datelor din Portugalia a aplicat o singură sancțiune cu amendă în cuantum de 400.000 de euro unui spital public din cauza măsurilor tehnice și organizatorice insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Investigația a dezvăluit faptul că personalul spitalului, psihologii, nutriționiștii și alți profesioniști au avut acces la datele pacienților prin profiluri false. Sistemul de management al profilurilor a fost deficient. Spitalul avea înregistrate 985 de profiluri de doctori, în timp ce în realitate existau doar 296 de doctori. Mai mult decât atât, membrii personalului aveau acces la dosarele pacienților, indiferent de specializarea lor.



DE REȚINUT! Pentru preîntâmpinarea unor prelucrări nelegale de date personale, compania trebuie să utilizeze o rețea sigură. Sigur

că pot interveni breșe de securitate, chiar dacă societatea îndeplinește condițiile optime în ceea ce privește componenta tehnică, de aceea trebuie avută în vedere instruirea periodică a persoanelor vizate, actualizarea datelor din toate sistemele, implicarea activă a DPO-ului etc.

România

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) a aplicat până la acest moment, în anul 2020, un număr total de 14 amenzi, iar în anul 2019 numărul total al amenzilor a atins 21. Temeiul principal avut în vedere pentru sancționarea operatorilor a fost insuficiența temeiurilor de prelucrare.

- o ANSPDCP a aplicat o amendă în cuantum de 2.000 de euro operatorului Viva Credit IFN SA pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea nu a răspuns solicitărilor persoanelor vizate în ceea ce privește exercitarea drepturilor GDPR. Mai concret, operatorului i-a fost solicitată exercitarea dreptului la ștergerea datelor, însă cererea nu a primit un feedback corespunzător.



DE REȚINUT! Operatorii trebuie să acorde foarte mare importanță solicitărilor primite din partea persoanelor vizate, și, în același timp, să dea curs unor astfel de solicitări. Întârzierile în astfel de cazuri sunt sancționate de către autoritate.

- o ANSPDCP a aplicat o amendă în cuantum de 2.000 de euro Poștei Române pentru insuficiența implementării măsurilor tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Concret, urmare a unei investigații întreprinse de autoritate, a fost arătat faptul ca numerele de telefon și adresele de e-mail ce aparțin unui număr de 81 de persoane vizate nu au fost pseudonimizate astfel încât să fie asigurată confidențialitatea.



DE REȚINUT! Operatorii trebuie să asigure implementarea unor măsuri tehnice și organizatorice adecvate pentru asigurarea protecției adecvate a datelor cu caracter personal prelucrate. În acest sens,

pseudonimizarea este un procedeu destul de des întâlnit care asigură că prin atribuirea unui alt element de identificare, persoana vizată nu poate fi individualizată într-un mod facil.

- o ANSPDCP a aplicat o amendă în cuantum de 5.000 de euro CNTAR Tarom SA pentru insuficiența implementării măsurilor tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Operatorul nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, fapt ce a condus la pierderea confidențialității datelor personale prin accesarea neautorizată a datelor aparținând unui număr de cinci pasageri TAROM, precum și la divulgarea neautorizată a datelor acestora.



DE REȚINUT! Măsurile tehnice și organizatorice includ și obligația operatorului de a asigura accesul la datele cu caracter personal exclusiv pentru persoanele ce îndeplinesc astfel de atribuții.

- o ANSPDCP a aplicat o amendă în cuantum de 15.000 de euro pentru Proleasing Motors SRL, motivul fiind măsurile tehnice și organizaționale insuficiente pentru securitatea informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea nu a reușit să adopte măsurile necesare pentru a asigura protecția datelor, ceea ce a dus la publicarea pe Facebook a unor documente ce conțineau parolele pentru accesul la datele personale a peste 436 de clienți.



DE REȚINUT! Operatorii trebuie să asigure măsuri de protecție adecvate pentru operațiunile de prelucrare a datelor cu caracter personal.

- o ANSPDCP a aplicat o amendă în cuantum de 15.000 de euro operatorului Enel Energie din cauza măsurilor tehnice și organizatorice insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Nu au fost luate măsuri adecvate pentru prevenirea dezvăluirii neautorizate a datelor personale. Amenda a fost precedată de o plângere privind dezvăluirea datelor personale ale unei persoane vizate unui alt client printr-un e-mail.



DE REȚINUT! Din nou se poate observa cum lipsa unei proceduri dedicate securității datelor a condus la sancționarea operatorului.

o ANSPDCP a dispus sancționarea operatorului Telekom Romania cu amendă în cuantum de 3.000 de euro din cauza măsurilor tehnice și organizatorice insuficiente pentru securitatea informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Măsurile de securitate inadecvate au dus la prelucrarea nelegală a datelor personale fără a fi verificată acuratețea lor. Pe lângă amendă, a fost impusă implementarea unui mecanism eficient de identificare și protejare a datelor împotriva dezvăluirii neautorizate și prelucrării nelegale.



DE REȚINUT! Este din nou adusa în discuție importanța implementării unor măsuri tehnice și organizatorice adecvate de către operatori, care în cazul de față a luat forma unei prelucrări de către persoane neautorizate.

o ANSPDCP a dispus sancționarea operatorului Banca Comercială Română SA cu amendă în cuantum de 5.000 de euro, motivul fiind măsurile tehnice și organizatorice insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Lipsa măsurilor adecvate a fost remarcată în special în colectarea și transmiterea copiilor documentelor de identificare a clienților prin Whatsapp.



DE REȚINUT! În cadrul operațiunilor de prelucrare trebuie să fie utilizate canale de comunicare ce îndeplinesc toate rigorile aferente securității datelor.

o ANSPDCP a aplicat o amendă în cuantum de 3.000 de euro companiei Estee Lauder Romania, motivat de insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost prelucrate fără o bază legală date personale, inclusive date medicale.



DE REȚINUT! Prelucrarea datelor cu caracter personal se poate face exclusiv în baza temeiurilor descrise de GDPR.

o ANSPDCP a dispus sancționarea operatorului Telekom Romania Communications SA cu amendă în cuantum de 3.000 de euro, motivul fiind măsurile tehnice și organizatorice insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea nu a adoptat suficiente măsuri pentru asigurarea acurateții datelor personale transmise prin telefon pentru încheierea contractelor, ceea ce a condus la încheierea contractelor prin telefon pe seama altor persoane.



DE REȚINUT! Operatorul trebuie să implementeze măsuri care să preîntâmpine astfel de incidente.

o ANSPDCP a aplicat o amendă în cuantum de 2.000 de euro asociației SOS Infertilitatea din cauza lipsei de cooperare cu autoritatea de supraveghere.

Situația de fapt ce a stat la baza aplicării sancțiunii: Asociația nu a pus la dispoziția ANSPDCP informațiile solicitate după ce a prelucrat date personale fără temeii.



DE REȚINUT! Cooperarea dintre entitatea controlată și autoritate este necesară și indispensabilă procedurii investigațiilor.

o ANSPDCP a sancționat operatorul Enel Energie cu amendă în cuantum de 3.000 de euro din cauza măsurilor tehnice și organizatorice insuficiente pentru securitatea informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea a trimis un e-mail unui client, conținând datele personale ale unui alt client.



DE REȚINUT! Este din nou punctată importanța implementării unor măsuri tehnice și organizatorice adecvate de către operatori.

o ANSPDCP a sancționat operatorul Vodafone Romania cu amendă în cuantum de 4150 de euro pe baza măsurilor tehnice și organizatorice insuficiente pentru a asigura securitatea informațiilor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea a trimis un e-mail unui client, conținând datele personale ale unui alt client.



DE REȚINUT! Acțiunile întreprinse de către operator nu se circumscriu sferei implementării unor măsuri tehnice și organizatorice adecvate.

o ANSPDCP a sancționat operatorul Dante International cu amendă în cuantum de 3.000 de euro, motivat de insuficiența temeiului de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Concret, societatea a trimis un e-mail în scop comercial unui client, deși clientul s-a dezabonat anterior de la mesajele comerciale.



DE REȚINUT! Prelucrarea datelor cu caracter personal se poate face exclusiv în baza temeiurilor descrise de GDPR, operatorul făcând dovada existenței acestora.

o ANSPDCP a dispus sancționarea Vodafone Romania cu amendă în cuantum de 3.000 de euro din cauza măsurilor tehnice și organizatorice insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Vodafone Romania a prelucrat incorect date personale ale unei persoane pentru a procesa o plângere al cărei răspuns a fost trimis ulterior la o adresă greșită de e-mail.



DE REȚINUT! Acțiunile întreprinse de către operator nu fac parte din sfera implementării unor măsuri tehnice și organizatorice adecvate.

o ANSPDCP a aplicat o amendă operatorului Telekom Romania Mobile Communications SA în cuantum de 2.000 de euro, motivul fiind reprezentat de măsurile tehnice și organizaționale insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea nu a asigurat acuratețea prelucrării datelor personale, ceea ce a permis dezvăluirea datelor personale ale unui client unui alt client.



DE REȚINUT! Astfel de acte precum cele promovate de operatorul menționat mai sus nu sunt conforme implementării măsurilor tehnice și organizatorice.

o ANSPDCP a aplicat o amendă societății Globus Score SRL în cuantum de 2.000 de euro pentru colaborarea insuficientă cu autoritatea de supraveghere, neexistând o conformare suficientă cu măsurile impuse de către ANSPDCP.



DE REȚINUT! Din nou, cooperarea dintre entitatea controlată și autoritate este necesară și indispensabilă procedurii investigațiilor. Lipsa cooperării poate conduce la sancțiuni.

- o ANSPDCP a dispus sancționarea operatorului Enel Energie S.A. (Electricity Distributor) cu amendă în cuantum de 6.000 de euro, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Sancțiunile au venit ca urmare a unei plângeri conform căreia Enel Energie a prelucrat în mod nelegal datele personale ale unei persoane și nu a putut demonstra faptul că obținuse consimțământul persoanei pentru a-i trimite notificări prin e-mail. În plus, Enel nu a luat măsurile necesare pentru a opri transmiterea notificărilor, deși persoana a obiectat în repetate rânduri. Operatorul a primit două sancțiuni, ambele în valoare de 3.000 de euro.



DE REȚINUT! Și în acest caz, a fost arătat faptul că prelucrarea datelor în temeiul dispozițiilor exprese GDPR este imperativ necesară.

- o ANSPDCP a dispus sancționarea societății Entirely Shipping & Trading S.R.L. cu amendă în valoare de 5.000 de euro, din cauza nerespectării principiilor generale pentru prelucrarea datelor.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea a prelucrat datele biometrice ale angajaților (amprente) pentru a accesa anumite camere, deși existau alte măsuri care să nu încalce atât de mult drepturile persoanelor respective.



DE REȚINUT! Unul dintre cele mai importante principii GDPR este principiul minimizării prelucrării datelor – presupune obligativitatea operatorului de a nu colecta date cu caracter personal care nu sunt necesare și de care se poate lipsi.

- o ANSPDCP a dispus sancționarea societății Entirely Shipping & Trading S.R.L. cu amendă în valoare de 5.000 de euro, motivul fiind nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a prelucrat în mod excesiv datele personale ale angajaților prin camerele video instalate în birouri și la vestiare, fiind încălcat principiul minimizării.



DE REȚINUT! Companiile trebuie să evite instalarea de mijloace de supraveghere video în birouri, toalete, vestiare sau orice alte locuri în care, în mod rezonabil, angajatul are nevoie de intimitate.

o ANSPDCP a sancționat Hora Credit IFN SA cu amendă în cuantum de 14.000 de euro, din cauza măsurilor tehnice și organizatorice insuficiente de asigurare a securității informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: A fost formulată o plângere conform căreia societatea a transmis documente ce conțineau date cu caracter personale ale altei persoane la o adresă de e-mail greșită. Cu ocazia investigației, s-a descoperit faptul că societatea prelucra date fără a asigura mecanisme eficiente pentru verificarea acurateții datelor colectate și nici nu a luat măsuri suficiente pentru asigurarea protecției datelor necesare pentru a evita accesul neautorizat al terților la datele personale. De asemenea, aceasta nu a notificat autoritatea de supraveghere privind breșa de securitate în termen de 72 de ore din momentul în care a cunoscut incidentul.



DE REȚINUT! Operatorul trebuie să acționeze imediat în cazul unei breșe de securitate, pasivitatea putând atrage o sancțiune mai aspră, mai ales în contextul în care obiectul breșei de securitate este reprezentat de date sensibile.

o ANSPDCP a dispus sancționarea operatorului SCNTAR TAROM SA (Airline), motivul fiind măsurile insuficiente de asigurare a securității informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea a fost sancționată, deoarece nu a adoptat măsurile adecvate pentru a asigura faptul că orice persoană fizică ce acționează sub supravegherea sa procesează datele conform instrucțiunilor sale. Astfel, un angajat a avut acces neautorizat la aplicația de rezervări și a putut fotografia o listă cu date personale ale 22 de pasageri, făcând publică lista pe Internet.



DE REȚINUT! Operatorul trebuie să fie proactiv și să implementeze măsuri menite să preîntâmpine astfel de incidente. Esențială este și instruirea angajaților care intră în contact cu datele personale.

o ANSPDCP a aplicat o amendă în cuantum de 2.000 de euro operatorului Nicola Medical Team 17 SRL din cauza cooperării insuficiente cu autoritatea de supraveghere.

o ANSPDCP a sancționat cu amendă în cuantum de 2.500 de euro operatorul Royal President SRL, motivul fiind nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea a refuzat o solicitare de acces la date personale și a dezvăluit date personale fără consimțământul persoanelor vizate. De asemenea, aceasta nu a adoptat măsuri adecvate pentru a asigura securitatea datelor prelucrate.



DE REȚINUT! Drepturile persoanelor vizate conform GDPR trebuie respectate cu prioritate de către operatori, iar solicitările trebuie tratate foarte atent astfel încât să se furnizeze un răspuns pozitiv sau după caz, negativ persoanei vizate privind exercitarea dreptului în cauză.

o ANSPDCP a dispus sancționarea unei asociații de proprietari cu suma de 500 de euro, motivul fiind insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Asociația a utilizat un sistem de supraveghere video fără o informare adecvată și fără măsuri de securitate privind persoanele care aveau acces la sistem.



DE REȚINUT! Companiile care utilizează sisteme de supraveghere video se vor asigura faptul că acestea sunt semnalizate corespunzător prin intermediul pictogramelor specifice și se vor asigura că durata de retenție este proporțională scopului în care sistemul a fost instalat.

o ANSPDCP a sancționat ING Bank N.V. cu amendă în cuantum de 80.000 de euro, motivul fiind lipsa măsurilor tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Banca nu a luat măsurile adecvate pentru sistemul de procesare automată a datelor personale în timpul procesului de decontare a tranzacțiilor cu cardul afectând 225.525 de clienți, ceea ce a condus la realizarea unor tranzacții duble între 8 și 10 octombrie.



DE REȚINUT! Operatorul trebuie să fie proactiv și să implementeze măsuri menite să preîntâmpine astfel de incidente. Esențială este și instruirea angajaților care intră în contact cu datele personale.

o ANSPDCP a aplicat o amendă în cuantum de 3.000 de euro operatorului Modern Barber, motivul fiind insuficienta cooperare cu autoritatea de supraveghere.



DE REȚINUT! După cum menționam și mai sus, cooperarea cu autoritatea în timpul unei investigații este foarte importantă, operatorul putând fi sancționat pentru lipsa de cooperare.

o ANSPDCP a dispus sancționarea unei companii de curierat cu suma de 11.000 de euro, motivul fiind insuficiența măsurilor tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Operatorul nu a reușit să adopte măsurile adecvate de protecție, ceea ce a condus la pierderea și accesul neautorizat la datele personale a aproximativ 1.100 de persoane (nume, cod CVV, adresa posesorului cardului, numărul cardului, CNP, seria și numărul buletinului, contul bancar).



DE REȚINUT! Operatorul trebuie să fie proactiv și să implementeze măsuri menite să preîntâmpine astfel de incidente.

o ANSPDCP a sancționat cu amendă în cuantum de 2.000 de euro operatorul BNP Paribas Personal Finance S.A., motivul fiind nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea nu a reacționat în termenul stabilit de GDPR la solicitările de ștergere a datelor.



DE REȚINUT! Operatorul trebuie să trateze cu prioritate solicitările privind exercitățile de drepturi ale persoanei vizate.

o ANSPDCP a sancționat cu amendă în cuantum de 2.500 de euro operatorul UTTIS INDUSTRIES SRL, motivul fiind neîndeplinirea obligațiilor de informare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Sancțiunea a fost aplicată deoarece operatorul de date nu a putut dovedi faptul că persoanele vizate au fost informate despre prelucrarea datelor personale (imagini prin sistemul de supraveghere video) încă din anul 2016. De asemenea, au fost dezvăluite CNP-urile angajaților prin afișarea raportului pentru un training autorizat și nu s-a putut dovedi legalitatea prelucrării CNP-urilor prin dezvăluire.



DE REȚINUT! Angajatorul va evita instalarea de mijloace de supraveghere video în cadrul birourilor, considerându-se de către autoritățile de supraveghere că acestea sunt de natură a aduce atingere dreptului la viață privată a persoanelor vizate. De asemenea, angajatorul va avea în vedere să informeze persoanele vizate cu privire la existența camerelor prin intermediul pictogramelor specifice și va afișa note de informare cu detaliile prelucrării.

o ANSPDCP a dispus aplicare unei sancțiuni cu amendă în cuantum de 150.000 de euro pentru operatorul Raiffeisen Bank SA, motivul fiind măsurile tehnice și organizaționale insuficiente pentru asigurare securității informației.

Situația de fapt ce a stat la baza aplicării sancțiunii: Banca a realizat evaluări pe baza datelor cu caracter personal ale persoanelor înregistrate pe platforma Vreau Credit, asigurate de către angajații platformei prin intermediul Whatsapp iar rezultatele au fost transmise ulterior către platformă prin aceleași mijloace de comunicare.



DE REȚINUT! Întotdeauna operatorul trebuie să se asigure că mijloacele prin intermediul cărora transmite date cu caracter personal sunt suficient de bine securizate.

o ANSPDCP a aplicat o amendă în cuantum de 9.000 de euro operatorului Inteligo Media SA, motivul fiind insuficiența temeiului legal de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Ca parte din procesul de înregistrare pe site-ul avocatnet.ro, operatorul a utilizat o casuță necompletată, prin intermediul căreia utilizatorii puteau declara dacă doresc sau nu să primească newsletter prin e-mail. Fără vreo acțiune în acest sens, acestea îi erau trimise utilizatorului.



DE REȚINUT! Compania trebuie să poate demonstra legalitatea comunicărilor realizate în scopuri de marketing. În acest sens se va face dovada consimțământului ori după caz, a existenței intereselor legitime ce au la bază relația relevantă dintre companie și persoana vizată.

o ANSPDCP a dispus sancționarea operatorului LEGAL COMPANY & TAX HUB SRL cu amendă în cuantum de 3.000 de euro, motivul fiind insuficiența măsurilor tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Lipsa măsurilor de securitate adecvate a condus la dezvăluirea neautorizată și accesul neautorizat la datele personale ale oamenilor care au făcut tranzacții primite de către site-ul avocatoo.ro (nume, prenume, adrese de e-mail, număr de telefon, job). Sancțiunea a fost aplicată în urma unei plângeri din 2018 conform căreia un set de documente privind detaliile tranzacțiilor primite de avocatoo.ro au fost accesibile în mod public prin 2 linkuri.



DE REȚINUT! Operatorul trebuie să implementeze măsuri menite să preîntâmpine astfel de incidente.

o ANSPDCP a aplicat o amendă în cuantum de 15.000 de euro operatorului WORLD TRADE CENTER BUCHAREST SA, motivul fiind insuficiența măsurilor tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Breșa de securitate a constat în faptul că o foaie utilizată pentru a nota clienții de la mic-dejun, conținând datele personale a 46 de clienți cazați, a fost fotografiată de către persoane neautorizate ce nu făceau parte din companie.



DE REȚINUT! Accesarea neautorizată a datelor cu caracter personal poate atrage răspunderea companiei, fiind esențială instruirea angajaților care intră în contact cu datele aparținând operatorului.

o ANSPDCP a dispus sancționarea operatorului UNICREDIT BANK SA cu o amendă în cuantum de 130.000 de euro, motivul fiind insuficiența măsurilor tehnice și organizatorice adecvate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost rezultatul lipsei măsurilor adecvate, ceea ce a condus la dezvăluirea online a cărților de identitate și a adreselor a 337.042 de persoane vizate.



DE REȚINUT! Operatorul de date, fie că face parte din sectorul public, fie că face parte din sectorul privat, trebuie să fie proactiv și să implementeze măsuri care să preîntâmpine astfel de incidente.

Slovacia

Autoritatea de supraveghere slovacă a aplicat un număr total de 6 amenzi pentru nerespectarea cerințelor GDPR, motivul principal constând în insuficiența măsurilor tehnice și organizatorice adecvate.

o Oficiul pentru Protecția Datelor din Slovacia a aplicat o sancțiune pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un operator de date nu a îndeplinit cererile persoanei vizate privind accesul la datele sale personale prelucrate prin intermediul unor înregistrări audio.



DE REȚINUT! Operatorul garantează accesul la date atunci când persoana vizată își exercită acest drept, punând la dispoziție copii de pe aceste date.

o Oficiul pentru Protecția Datelor din Slovacia a aplicat o amendă pentru insuficiența măsurilor tehnice și organizatorice implementate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost dezvăluite documente conținând date personale în zona gropii de gunoi a orașului.



DE REȚINUT! Anterior predării către o societatea specializată a documentelor confidențiale pentru care a expirat perioada de retenție sau a oricăror alte tipuri de documente ce conțin date personale sau după caz, anterior aruncării lor, se recomandă ca acestea să fie introduse într-un shredder, pentru a preîntâmpina orice incident de securitate derivat din accesarea neautorizată a datelor.

o Oficiul pentru Protecția Datelor din Slovacia a dispus aplicarea unei sancțiuni, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost publicate nelegal date personale pe site-ul unui oraș în cadrul îndeplinirii obligației sale de divulgare în temeiul Legii privind libertatea informațiilor. Totuși, autoritatea a considerat faptul că orașul a publicat datele încălcând legea și fără acordul persoanelor respective.



DE REȚINUT! Operatorul, fie că face parte din sectorul privat, fie că face parte din sectorul public, se va asigura că temeiul de prelucrare utilizat este acoperitor în ceea ce privește procesele de prelucrare avute în vedere.

o Oficiul pentru Protecția Datelor din Slovacia a dispus aplicarea unei sancțiuni operatorului Slovak Telekom cu amendă în cuantum de 40.000 de euro pentru insuficiența măsurilor de securitatea implementate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Operatorul nu a adoptat măsurile de securitate adecvate pentru prelucrarea datelor, încălcând astfel obligația de a proteja prelucrarea datelor.

o Oficiul pentru Protecția Datelor din Slovacia a aplicat o amendă în cuantum de 50.000 de euro, motivul fiind insuficiența măsurilor tehnice și organizatorice implementate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Aplicațiile pentru ajutoarele sociale completate de cetățeni slovaci au fost trimise prin poștă autorităților străine. Acestea au fost pierdute de către poștă, datele nemaiputând fi localizate.



DE REȚINUT! Operatorul de date trebuie să depună toate diligențele, astfel încât să prevină incidentele de securitate precum pierdere, furt etc.

Spania

În Spania au fost date peste 117 amenzi de către Agenția Spaniolă pentru Protecția Datelor – AEPD. Având în vedere numărul mare, vom analiza doar o parte dintre acestea în cazul cărora AEPD a menționat anumite aspecte de interes.

În anul 2020, autoritatea spaniolă de supraveghere (AEPD) a dispus sancționarea a peste 70 de operatori:

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a sancționat operatorul El Periódico de Catalunya, S.L.U. cu amendă în cuantum de 10.000 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: După ce și-a exercitat dreptul la ștergere, o persoană vizată a primit mesaje de marketing de la publicație. Motivul transmiterii mesajelor nesolicitate a constat în erorile care au intervenit din partea furnizorului extern pentru aceste servicii.



DE REȚINUT! Pentru a preîntâmpina astfel de situații, operatorul trebuie să se asigure că împuterniciții pot furniza servicii GDPR compliant, asumându-și o eventuală sancțiune ce ar putea fi aplicată în cazul în care acest furnizor nu respectă cerințele legale.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a sancționat operatorul Asociación de Médicos Demócratas cu amendă în cuantum de 10.000 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Organizația a prelucrat date ale membrilor fără a avea consimțământul acestora.



DE REȚINUT! În funcție de procesul de prelucrare, temeiul legal avut în vedere poate fi unul diferit. Dacă organizația poate avea anumite obligații legale cu privire la colectarea anumitor date, pentru anumite procese de prelucrare se va baza pe consimțământ sau pe interesele legitime ale operatorului.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a aplicat o amendă în cuantum de 24.000 de euro operatorului Iberdrola Clientes pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: O terță persoană a primit o factură pentru electricitate cu date personale, precum nume, adresă și conturi bancare ale unui alt client, din cauza faptului că nu au fost implementate măsuri adecvate de securitate, încălcând principiile de integritate a datelor și de confidențialitate.



DE REȚINUT! Este în sarcina operatorului să preîntâmpine astfel de incidente. Neimplementarea măsurilor tehnice și organizatorice necesare poate conduce la sancțiuni în ceea ce privește persoana operatorului în măsura în care acesta nu implementează un sistem prin intermediul căruia să fie stabilit concret unde ajung sau pot ajunge datele clienților.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a dispus sancționarea operatorului Brigada Națională de Poliție cu amendă în cuantum de 6.000 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: În cadrul unei investigații, s-au făcut copii ale registrelor aparținând unei companii ce conțineau date ale unor terți, neexistând o bază legală de prelucrare.



DE REȚINUT! Operatorul, de această dată un organism al statului, a efectuat operațiuni de prelucrare fără a analiza existența temeiului legal al prelucrării. Or, așa cum arătam anterior, în contextul analizei altor sancțiuni similare, este de avut în vedere faptul că nu prezintă relevanță faptul că operatorul provine din sectorul privat sau public, acesta având aceleași obligații legale impuse de GDPR față de persoanele vizate.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a sancționat cu amendă în cuantum de 2.000 de euro o cafenea pentru nerespectarea principiilor legale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost folosite mijloace de supraveghere video fără a exista o informare a persoanelor vizate.



DE REȚINUT! Companiile care utilizează sisteme de supraveghere video se vor asigura faptul că acestea sunt semnalizate corespunzător prin intermediul pictogramelor specifice și se vor asigura că durata de retenție este proporțională scopului în care sistemul a fost instalat.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a aplicat o amendă în cuantum de 75.000 de euro companiei Xfera Moviles S.A., motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Persoana vizată a primit o notificare de la o companie de recuperare creanțe, fiindu-i solicitate plăți pentru serviciile Xfera Mobiles, deși reclamantul nu mai fusese clientul acesteia încă din septembrie 2017. De asemenea, Xfera Moviles a prelucrat datele sale personale fără acordul său.



DE REȚINUT! Operatorul trebuie să se asigure că orice divulgare de date este acoperită de un temei legal, existând riscul, în caz contrar, să se considere că a avut loc o încălcare a prevederilor legale în materie de prelucrare de date.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a dispus sancționarea cu amendă în cuantum de 5.000 de euro a operatorului Consulting de Seguridad e Investigacion Mira Dp Madrid S.L., motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: O persoană a primit mesaje de marketing fără consimțământul său.



DE REȚINUT! Prelucrarea datelor cu caracter personal în scop de marketing (astfel cum a fost cazul mai sus) poate avea loc, ca regulă generală, în baza consimțământului expres și în anumite cazuri excepționale, în baza intereselor legitime ale operatorului.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a aplicat o amendă în cuantum de 75.000 de euro operatorului Equifax Iberica, S.L. pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Persoana vizată a solicitat prin e-mail ștergerea datelor sale din dosarul Asociației Naționale

a Instituțiilor Financiare de Credite. Compania a răspuns că exercitarea dreptului persoanei respective a fost excesivă din cauza unei cereri anterioare și că nu se vor șterge datele.



DE REȚINUT! Operatorii trebuie să fie foarte atenți atunci când primesc solicitări din partea persoanelor vizate, conținând exercitarea drepturilor prevăzute de GDPR. Un eventual refuz poate fi justificat strict prin raportare la prevederile legale.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a aplicat o amendă în cuantum de 25.000 de euro operatorului Glovoapp23 pentru lipsa unui DPO.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea nu a numit un DPO căruia să îi fie adresate solicitările persoanelor vizate și site-ul nu conținea alte informații privind acest subiect.



DE REȚINUT! GDPR nu prevede expres cazurile în care este necesară desemnarea DPO-ului, fiind necesar ca operatorul să realizeze dacă realizează prelucrări sistematice sau pe scară largă. Cu toate acestea, acolo unde volumul de date este foarte mare (magazine online, unități de cazare, școli, grădinițe, spitale/clinici etc.), este recomandat ca numirea DPO-ului să fie o prioritate.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a dispus sancționarea operatorului Shop Macoyn, S.L. cu amendă în cuantum de 5.000 de euro, motivul fiind insuficiența măsurilor tehnice și organizatorice.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost trimise mai multe e-mail-uri cu reclame mai multor destinatari, fiind vizibile adresele de e-mail ale tuturor destinatarilor, din cauza faptului că au fost introduse în secțiunea cc, nu bcc.



DE REȚINUT! Companiile, în calitatea lor de operatori de date, trebuie să prevină astfel de incidente. Esențială în acest sens este instruirea periodică a angajaților care gestionează datele personale, astfel încât aceștia să fie responsabilizați în mod corespunzător.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a sancționat cu amendă în cuantum de 1.000 de euro operatorul Cerrajería Verin S.L., motivul fiind neîndeplinirea obligației de informare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Operatorul a colectat date personale fără să fie oferite în politica de confidențialitate de pe site informații despre activitățile de prelucrare.



DE REȚINUT! Deși majoritatea companiilor privesc politica de confidențialitate ca un document standard ce nu impune particularități, practica autorităților demonstrează faptul ca operatorii trebuie să acorde o importanță sporită atât politicii de confidențialitate sau de prelucrare, cât și politicii de cookies, care au rolul de a informa persoanele vizate cu privire la prelucrările de date prin intermediul site-ului. Un principiu important ce stă la baza GDPR este acela al transparenței. Conform acestui principiu, operatorii trebuie să informeze în mod concret care sunt datele prelucrate, temeiul prelucrării și alte asemenea informații.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a aplicat o amendă în cuantum de 60.000 de euro unei societăți de televiziune, motivul fiind reprezentat de măsurile tehnice și organizatorice insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Societatea a raportat breșa de securitate la AEPD după ce 6 stick-uri USB necriptate ce conțineau date personale au fost pierdute, ceea ce a afectat aproximativ 11.000 de persoane, fiind vorba de date precum cele de identificare, de angajare, medicale sau cazier.



DE REȚINUT! Raportarea unor astfel de breșe de securitate trebuie realizată fără întârzieri autorității conform dispozițiilor GDPR. Se recomandă ca, în analiza incidentului de securitate, să fie implicat și DPO-ul.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a dispus sancționarea operatorului Xfera Moviles S.A. cu amendă în cuantum de 60.000 de euro, motivul fiind insuficiența măsurilor de securitate implementate.

Situația de fapt ce a stat la baza aplicării sancțiunii: O persoană a primit un mesaj din partea societății ce trebuia adresat unui terț, fapt care i-a permis să acceseze contul și datele terțului pe site-ul companiei, prin intermediul unui număr de telefon și unei parole primite prin SMS.



DE REȚINUT! Operatorii de date trebuie să acorde o importanță deosebită implementării măsurilor tehnice și organizatorice al căror rol este acela de a preveni incidente precum cel de mai sus.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a sancționat operatorul LaLiga, o liga profesionistă de fotbal din Spania, cu amendă în cuantum de 250.000 de euro pentru neîndeplinirea obligațiilor legale de informare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Liga de fotbal a fost amendată pentru oferirea unei aplicații care accesa o data pe minut microfonul utilizatorilor telefonului mobil pentru a detecta pub-urile ce difuzează meciuri fără a plăti taxele. LaLiga nu a informat adecvat utilizatorii aplicației despre această practică. De asemenea, aplicația nu îndeplinea cerințele pentru retragerea consimțământului.



DE REȚINUT! Operatorii de date cu caracter personal trebuie să informeze în mod obligatoriu în prealabil persoanele vizate despre prelucrarea datelor și să ofere instrumente adecvate de retragere a consimțământului.

o Agenția Spaniolă pentru Protecția Datelor (AEPD) a dispus sancționarea Vodafone España, S.A.U. cu amendă în cuantum de 40.000 de euro pentru lipsa implementării unor măsuri tehnice și organizatorice corespunzătoare.

Situația de fapt ce a stat la baza aplicării sancțiunii: A fost taxat un serviciu Netflix care nu fusese solicitat de către reclamant, care a putut dovedi faptul că serviciul a fost folosit de către altcineva care primise contul său bancar și numărul lui telefon de la Vodafone. Din moment ce compania nu a putut dovedi faptul că persoana respectivă și-a dat consimțământul pentru încheierea contractului privind serviciul Netflix, AEPD a aplicat amenda menționată mai sus.



DE REȚINUT! Neimplementarea măsurilor tehnice și organizatorice poate conduce la dificultăți cu privire la administrarea bazei de date și prelucrarea datelor aferente. În cazul de mai sus, lipsa implementării măsurilor a condus la divulgarea neautorizată a datelor cu caracter personal.

Suedia

Autoritatea suedeză de supraveghere a datelor a aplicat un număr total de 6 amenzi, principalul aspect sancționat constând în insuficiența temeiului de prelucrare.

În anul 2020 au fost aplicate 4 amenzi pentru nerespectarea GDPR:

- o Autoritatea de supraveghere din Suedia a sancționat o asociație de locuințe cu amendă în cuantum de 1.900 de euro, motivul fiind nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost utilizate în mod nelegal camere de supraveghere video. În decizie, autoritatea de supraveghere a specificat faptul că înregistrările audio au implicări adiționale de confidențialitate, în special pentru clădirile rezidențiale și că în cazul acesta nu exista nimic care să justifice înregistrarea. În plus, decizia cere asociației să înceteze înregistrarea scărilor și intrărilor, să oprească înregistrarea audio și să îmbunătățească informarea despre camerele de supraveghere.



DE REȚINUT! Operatorul care utilizează sisteme de supraveghere video se va asigura de faptul că acestea sunt semnalizate corespunzător prin intermediul pictogramelor specifice și se va asigura că durata de retenție este proporțională scopului în care sistemul a fost instalat.

- o Autoritatea de supraveghere din Suedia a dispus sancționarea Consiliului medical și de sănătate al regiunii județului Örebro cu amendă în cuantum de 11.200 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Au fost publicate datele personale ale unui pacient fără a avea o bază legală.



DE REȚINUT! Operatorul trebuie să se asigure de existența temeiului legal pentru toate procesele de prelucrare pe care le are în vedere.

- o Autoritatea de supraveghere din Suedia a aplicat o amendă în cuantum de 18.700 de euro operatorului Centrului Național de servicii guvernamentale pentru neîndeplinirea obligațiilor legale privind notificarea breșelor de securitate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Decizia autorității de supraveghere arată faptul că a durat aproape 5 luni până când operatorul a notificat persoanele implicate breșa de securitate și aproape 3 luni până a primit autoritatea notificarea.



DE REȚINUT! În cazul unei breșe de securitate, operatorul trebuie să reacționeze prompt și să notifice autoritatea de supraveghere în termen de 72 de ore.

o Autoritatea de supraveghere din Suedia a dispus sancționarea operatorului Google LLC cu amendă în cuantum de 7.000.000 de euro, motivul fiind nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Google a primit amenda pentru că nu s-a conformat în mod corespunzător cu obligațiile sale referitoare la dreptul persoanelor vizate de a li se șterge rezultatele căutărilor din lista de rezultate.



DE REȚINUT! Conform CJUE, operatorul unui motor de căutare pe internet răspunde pentru prelucrarea pe care o efectuează în ceea ce privește datele cu caracter personal care apar pe pagini web publicate de terți.

În anul 2019 au fost aplicate 2 amenzi pentru nerespectarea GDPR:

o Autoritatea de supraveghere din Suedia a dispus sancționarea operatorului Nusvar AB cu amendă în cuantum de 35.000 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania, operator al site-ului Mrkoll.se, care furnizează informații despre toți cetățenii Suediei cu vârsta peste 16 ani, a publicat informații despre oameni care au întârzieri la plăți.



DE REȚINUT! Operatorul trebuie să se asigure că temeiul prelucrării este acoperitor pentru toate procesele de prelucrare și cu privire la toate categoriile de date.

o Autoritatea de supraveghere din Suedia a dispus sancționarea unei școli din Skellefteå cu amendă în cuantum de 18.630 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Școala a făcut o încercare pentru utilizarea tehnologiei de recunoaștere facială. Amenda a fost impusă pentru utilizarea tehnologiei pentru monitorizarea prezenței elevilor. Deși, în general, prelucrarea datelor cu scopul de monitoriza prezența este posibilă, utilizarea acestei tehnologii pentru acest scop este disproporționată. Autoritatea de supraveghere consideră că datele

biometrice ale elevilor au fost astfel prelucrate excesiv. Mai mult decât atât, argumentul conform căruia exista consimțământ nu se poate aplica, din moment ce elevii și reprezentanții lor legali nu puteau decide în mod liber dacă vor sau nu să fie monitorizați în scop de evidență a prezenței. Autoritatea a descoperit faptul că era un caz de prelucrare cu riscuri ridicate, având în vedere faptul că noua tehnologie a fost utilizată pentru a prelucra date sensibile ale copiilor, care sunt într-o relație de dependență față de școală, fiind utilizate și camere de supraveghere în mediul de zi cu zi al elevilor. Școala nu a putut demonstra respectarea GDPR.



DE REȚINUT! Relațiile de dependență ridică probleme în analiza consimțământului. În mod similar copiilor care sunt dependenți de unitatea de învățământ și drept urmare, sunt nevoiți să își dea acordul pentru monitorizarea prezențelor cu ajutorul datelor biometrice. La fel se pune problema și în cadrul relațiilor de muncă acolo unde se prezumă că, dată fiind relația de subordonare, salariatul nu ar putea refuza să își exprime consimțământul. Cu toate acestea, dacă retragerea consimțământului ar fi garantată de către operator și i s-ar da în mod real eficiență, apreciem că un astfel de consimțământ ar putea fi valid.

Ungaria

Autoritatea ungară a aplicat un număr total de 28 de amenzi, principalele aspecte sancționate constând în insuficiența temeiului legal de prelucrare, nerespectarea principiilor generale de prelucrare și nerespectarea drepturilor persoanelor vizate.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a sancționat operatorul Digi Távközlési Szolgáltató Kft. („Digi”) cu amendă în cuantum de 288.000 de euro pentru măsurile de securitate a informației insuficiente.

Situația de fapt ce a stat la baza aplicării sancțiunii: Compania a încălcat principiile limitării scopului și restricționării stocării deoarece baza de date conținea un număr mare de date ale clienților care nu mai erau relevante pentru scopul actual al prelucrării și pentru care nu a fost setată o perioadă de retenție. Autoritatea a arătat faptul că nu au fost luate măsuri proporționale pentru a reduce riscurile privind securitatea și managementul datelor, argumentând, printre altele, că nu a fost folosit un mecanism de criptare.



DE REȚINUT! Un aspect foarte important de care companiile trebuie să țină cont este durata de retenție, atât cea impusă prin diverse acte normative, cât și cea stabilită intern, prin intermediul propriilor proceduri implementate în cadrul proceselor de conformare.

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus sancționarea unei bănci cu amendă în cuantum de 2.890 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Din cauza unor greșeli administrative, datele personale ale unei persoane au fost înregistrate și transferate către Sistemul Central de Informații de Credit în legătură cu un contract de împrumut, fără ca persoana respectivă să fie parte în acel contract.



DE REȚINUT! Operatorul trebuie să depună toate diligențele astfel încât să preîntâmpine astfel de incidente.

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus sancționarea unei companii cu amendă în cuantum de 5.800 de euro pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Operatorul de date nu s-a conformat cu obligațiile sale referitoare la dreptul de acces la înregistrările video și nu a putut demonstra că activitățile de prelucrare au fost în conformitate cu reglementările legale.

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus sancționarea unui creditor cu amendă în cuantum de 870 de euro pentru insuficiența temeiului legal al prelucrării.

Situația de fapt ce a stat la baza aplicării sancțiunii: A fost trimis un mesaj unui debitor pentru a-i aminti despre existența unei datorii, deși aceasta fusese deja plătită.



DE REȚINUT! Operatorul trebuie să depună toate diligențele pentru a evita astfel de incidente.

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a aplicat o amendă de 290 de euro unui

reprezentant al unei autorități locale, motivul fiind baza legală de prelucrare insuficientă.

Situația de fapt ce a stat la baza aplicării sancțiunii: Reprezentantul autorității locale a făcut o fotografie directorului unei companii deținute de autoritatea locală în care se vedea cum directorul rupe un afiș electoral al opoziției în prezența copilului său. Acesta a postat fotografia pe pagina sa de Facebook. Imaginea copilului a fost făcută neclară, dar a fost indicat în postare faptul că era vorba despre fiica directorului. Directorul a spus reprezentantului autorității locale că nu este de acord să i se facă poza. Autoritatea de supraveghere a considerat faptul că acțiunea directorului nu a fost una de informație publică, având această natură doar numele directorului.



DE REȚINUT! Libertatea de exprimare trebuie să fie corelată cu principiile generale și temeiurile prelucrării. Într-un astfel de material, puteau fi blurate sau chiar eliminate secvențe care ajutau la identificarea persoanelor vizate.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a sancționat o societate care furnizează servicii de contabilitate cu amendă în cuantum de 1.450 de euro pentru insuficiența măsurilor tehnice.

Situația de fapt ce a stat la baza aplicării sancțiunii: O listă de clienți printată ce conținea inclusiv date personale a putut fi accesată de persoane neautorizate.



DE REȚINUT! Accesarea neautorizată a datelor cu caracter personal poate atrage răspunderea companiei, fiind esențială instruirea angajaților care intră în contact cu datele aparținând operatorului.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus sancționarea unui operator cu amendă în cuantum de 1.430 de euro pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Angajatorul a restaurat căsuța de mailuri a unui director care a plecat din companie cu un an înainte și a găsit un e-mail ce conținea documente legate de muncă. Directorul nu a primit nicio avertizare că va fi activat acest mail și nu a avut șansa să copieze sau să șteargă datele personale (parole, informații financiare). Conform autorității, un angajat sau reprezentant ar trebui să fie

B.C.U. „M. EMINESCU” IAȘI

ȘTIINȚE ECONOMICE

prezent atunci când sunt prelucrate datele personale ale angajatului, chiar dacă contractul de muncă este încetat. Angajatorii trebuie să înregistreze accesul cu minute și fotografiile când angajatul nu poate fi prezent și în prezența martorilor independenți. Angajatorii trebuie să adopte politici interne privind arhivarea și utilizarea activelor IT și a conturilor de e-mail, inclusiv norme procedurale, cum ar fi etapele unei inspecții și angajații autorizați să o efectueze.



DE REȚINUT! În cadrul relațiilor de muncă drepturile fostului angajat persoană vizată subzistă și după încetarea contractului de muncă.

- Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a sancționat un spital pentru îndeplinirea insuficientă a obligațiilor de notificare a breșelor de securitate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Spitalul nu a respectat termenul pentru notificarea breșei de securitate privind datele personale.



DE REȚINUT! Operatorul trebuie să acționeze imediat în cazul unei breșe de securitate, pasivitatea putând atrage o sancțiune mai aspră, mai ales în contextul în care obiectul breșei de securitate este reprezentat de date sensibile.

- Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a sancționat cu amendă în cuantum de 2.960 de euro o companie, motivul fiind nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un angajat a fost în concediu medical atunci când angajatorul său a verificat desktopul, laptopul și e-mailurile pentru a se asigura că sarcinile sale de muncă erau acoperite în absența sa. Angajatorul și-a suspendat apoi contul. Angajatul nu a primit o notificare prealabilă și nu a avut șansa de a copia / șterge informațiile sale private (numere de telefon, mesaje). Potrivit NAIH, angajatorii trebuie să înregistreze accesul cu minute și fotografiile. Acordurile de muncă trebuie să reglementeze dacă angajații pot folosi echipamentele de lucru în scopuri private. Notificările de confidențialitate trebuie să conțină motivele monitorizării angajaților (de exemplu, continuitatea activității, investigarea internă, scopurile disciplinare și perioada specifică de păstrare a datelor angajaților – inclusiv durata și

reapariția copiilor de rezervă. Angajatorii trebuie să pregătească „teste de echilibrare”) pentru a demonstra legitimitatea intereselor.



DE REȚINUT! În cadrul relațiilor de muncă drepturile fostului angajat persoană vizată subzistă și după încetarea contractului de muncă.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus o amendă în cuantum de 15.100 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Orașul și-a fundamentat practica de supraveghere video pe interesele sale legitime. Totuși, această bază legală nu se aplică prelucrării realizate de autoritățile publice în exercitarea atribuțiilor.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a aplicat o amendă în cuantum de 1.715 euro pentru nerespectarea principiilor legale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Proprietarii unei proprietăți imobiliare s-au plâns că biroul guvernamental și-a postat decizia privind schimbarea persoanei chiriașului (care a încheiat un contract de închiriere cu proprietarii imobiliari) pentru alți proprietari ai 40 de proprietăți imobiliare contractate de aceeași persoană. Decizia conținea date personale ale tuturor proprietarilor, care aveau un contract de închiriere cu aceasta.



DE REȚINUT! Operatorul se va asigura de faptul că temeiul de prelucrare este acoperitor în ceea ce privește toate procesele de prelucrare avute în vedere de operator.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus o amendă în cuantum de 4.290 de euro unei societăți ce furniza servicii de mentenanță a spațiului public pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un fost angajat s-a plâns cu privire la faptul că angajatorul său i-a monitorizat în mod ilegal activitatea prin intermediul mijloacelor de supraveghere video. Angajatorul a susținut că monitorizarea CCTV a fost necesară pentru a evalua dacă angajatul și-a îndeplinit îndatoririle legate de angajare (adică monitorizarea anumitor zone publice și semnalarea unui eveniment neobișnuit către colegii săi) și că monitorizarea a servit, de asemenea, la protecția sistemului său de supraveghere împotriva accesului sau utilizării ilegale. NAIH

a constatat că monitorizarea angajaților prin intermediul CCTV nu este o modalitate adecvată de evaluare a performanței de muncă, iar angajatorul nu avea o bază legală de prelucrare. Angajatorul ar fi putut proteja sistemul său de supraveghere a zonei publice prin alte metode (de exemplu, instalând firewall-uri sau alte îmbunătățiri de securitate la sistemele sale). Angajatorul a pus, de asemenea, doar o informare scurtă la intrarea în stația de lucru a salariatului cu privire la monitorizarea CCTV, pe care NAIH a considerat-o insuficientă.



DE REȚINUT! Recomandat este ca operatorii să nu se limiteze la afișarea pictogramelor specifice în materie de informare cu privire la existența mijloacelor de supraveghere video.

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a sancționat Budapest Environs Regional Court cu amendă în cuantum de 8.575 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Președintele Curții Regionale de la Budapesta a organizat o întâlnire pentru funcționarii judecătorești, în cadrul căreia a declarat că a renunțat la Asociația Maghiară a Judecătorilor și le-a solicitat să-i convingă și pe colegii lor să o facă. De asemenea, președintele a prezentat o listă cu membrii Asociației din județul Pest, care a inclus și informații despre cuantumul taxelor de membru deduse din salariul judecătorilor. Lista era formată din date culese din evidența salarizării judecătorilor. NAIH a stabilit că aceste date puteau fi prelucrate numai în scopul deducerii și administrării salarizării. NAIH a stabilit, de asemenea, că nu exista o bază legală pentru prelucrarea datelor, când s-a oferit acces la datele angajaților cu privire la apartenența lor la o asociație, altor persoane.

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a aplicat o amendă în cuantum de 2.850 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Persoana fizică a solicitat ștergerea datelor sale de contact (inclusiv numărul său de telefon), iar operatorul a prelucrat în continuare datele sale de contact în scopul executării cererilor pe baza interesului său legitim. NAIH a stabilit că operatorul nu are motive legitime convingătoare pentru prelucrarea numărului de telefon al persoanei vizate, întrucât adresa sa de e-mail era disponibilă, ceea ce este suficient pentru scopurile de executare a cererilor și pentru comunicarea cu persoana vizată.



DE REȚINUT! Dacă persoana vizată a oferit un consimțământ general pentru marketing (recomandat ar fi să vizeze canalele), operatorul va avea în vedere canalul care ar putea fi cel mai puțin deranjant pentru persoana vizată.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a aplicat o amendă în cuantum de 2.850 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un client al unei întreprinderi financiare a reclamat faptul că aceasta i-a transferat datele după ce s-a opus prelucrării și nu i-a furnizat informații cu privire la prelucrarea datelor sale la cererea sa. Potrivit întreprinderii financiare, acesta și-a vândut creanța provenind din contractul încheiat cu clientul său către un terț, prin urmare, o astfel de tranzacție a necesitat transferul datelor relevante ale clientului. NAIH a subliniat că întreprinderea financiară a vândut creanța aferentă și a transferat datele respective după neîndeplinirea contractului aferent de către client. Acest lucru înseamnă, de asemenea, că întreprinderea financiară nu se poate baza pe executarea contractului încheiat cu clientul. Baza legală relevantă ar fi fost interesul legitim al operatorului, unde este de asemenea necesar un test de echilibrare, care să descrie interesul său pentru a transfera cererea și datele relevante către o terță parte.



DE REȚINUT! Transferul datelor în vederea recuperării creanțelor în realizarea intereselor legitime ale operatorului presupune nu doar efectuarea unei LIA, ci și informarea corespunzătoare a persoanei vizate.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a aplicat o amendă în cuantum de 15.150 de euro pentru neîndeplinirea obligațiilor de notificare a breșelor de securitate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Operatorul de date nu a îndeplinit obligația de notificare atunci când o memorie externă ce conținea date personale a fost pierdută.



DE REȚINUT! Operatorul trebuie să preîntâmpine incidente precum pierdere, furt, atac etc.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus sancționarea unei firme de administrare a revendicărilor cu amendă în cuantum de 2.850 de euro, motivat de insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Reclamanții au declarat că au încheiat un contract de credit cu banca, care și-a vândut creanța împotriva reclamanților și a transferat datele respective către o companie. NAIH a stabilit că operatorul nu se poate baza nici pe consimțământul persoanelor vizate, nici pe executarea contractului de credit ca bază legală a prelucrării datelor, deoarece persoanele vizate au încheiat un astfel de contract cu banca, nu cu operatorul. Baza legală adecvată pentru prelucrare ar fi putut fi interesul legitim al operatorului.



DE REȚINUT! Transferul datelor în vederea recuperării creanțelor în realizarea intereselor legitime ale operatorului presupune nu doar efectuarea unei LIA, ci și informarea corespunzătoare a persoanei vizate.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a aplicat o amendă în cuantum de 2.000 de euro unei bănci pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Clientul unei bănci locale a solicitat accesul la înregistrările de conversații telefonice, precum și la înregistrările camerelor de supraveghere video. Banca a furnizat copii ale înregistrărilor convorbirilor telefonice și a oferit, de asemenea, șansa de a revizui înregistrările la bancă, dar a respins furnizarea de copii ale înregistrărilor CCTV, deoarece înregistrările conțineau și date personale ale terților. NAIH a decis în acest caz că banca nu a îndeplinit drepturile persoanelor vizate, întrucât nu a răspuns la termen și nu a furnizat, de asemenea, copii ale înregistrărilor solicitate.



DE REȚINUT! În astfel de situații, operatorul ar putea să ofere acces la materialele rezultate din supravegherea video, anonimizând părțile care ar putea conduce la identificarea unor terțe persoane.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus o amendă operatorului SZIGET festival și VOLT festival în cuantum de 92.146 de euro, motivul fiind insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: NAIH a constatat că nu există temei juridic corespunzător și că operatorul nu respectă

principiul limitării scopului. De asemenea, informațiile referitoare la prelucrarea datelor nu au fost complet furnizate persoanelor vizate.



DE REȚINUT! Operatorul se va limita în colectarea datelor strict la ceea ce este necesar în vederea prelucrării, neputând opta pentru modificarea scopului cu privire la care a informat persoana vizată.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a sancționat Direcția instituției sociale și de protecție a copilului din districtul Ferencváros din Budapesta cu amendă în cuantum de 286 de euro, motivul fiind îndeplinirea insuficientă a obligațiilor de notificare a breșelor de securitate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Angajatul Direcției a trimis din greșeală 9 scrisori către alți destinatari, care conțineau date personale ale 18 persoane vizate (inclusiv date despre copii, date penale și date referitoare la viața privată a persoanelor vizate). Destinatarul a informat Direcția după 5 zile că a primit din greșeală scrisorile. Direcția a notificat NAIH cu privire la încălcarea datelor câteva săptămâni mai târziu.



DE REȚINUT! În cazul unei breșe de securitate operatorul trebuie să reacționeze prompt și să notifice autoritatea de supraveghere în termen de 72 de ore.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus sancționarea cu amendă în cuantum de 9.400 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Un operator de date a utilizat, în opinia NAIH, un temei juridic greșit pentru prelucrarea datelor cu caracter personal pentru repartizarea cererilor de despăgubire.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a aplicat o sancțiune în cuantum de 34.375 de euro unui partid politic, motivul fiind îndeplinirea insuficientă a obligațiilor de notificare a breșelor de securitate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Partidul nu a notificat NAIH și persoanelor relevante o încălcare a securității datelor și nu a documentat încălcarea. Încălcarea a fost rezultatul unui atac cibernetic al unui hacker anonim care a accesat și dezvăluit informații despre vulnerabilitatea sistemului organizației – o bază de date de peste 6.000 de persoane. Sistemul a fost vulnerabil la atac din cauza unei

probleme de redirecționare cu pagina web a organizației. După ce atacatorul a publicat informațiile, chiar și persoane ce aveau cunoștințe IT scăzute au putut prelua informații din baza de date.



DE REȚINUT! În cazul unei breșe de securitate operatorul trebuie să reacționeze prompt și să notifice autoritatea de supraveghere în termen de 72 de ore.

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus aplicarea unei amenzi în cuantum de 1.900 de euro pentru nerespectarea dreptului de acces exercitat de către o persoană vizată.

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a sancționat o instituție financiară cu amendă în cuantum de 3.200 de euro pentru nerespectarea drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată în legătură cu solicitarea unei persoane pentru corectarea și ștergerea datelor. NAIH a aplicat o amendă împotriva instituției financiare pentru că a respins în mod ilegal cererea unui client de a-și șterge numărul de telefon după ce a susținut că este în interesul legitim al companiei să proceseze aceste date pentru a aplica o cerere de creanță împotriva clientului. În decizia sa, NAIH a subliniat că numărul de telefon al clientului nu este necesar în scopul colectării datoriilor, deoarece creditorul poate comunica cu debitorul prin poștă. În consecință, păstrarea numărului de telefon nu a respectat principiile minimizării datelor și limitării scopului.



DE REȚINUT! În astfel de situații, operatorul va da curs cererii persoanei vizate dacă există detalii care pot ajuta la comunicarea persoanei vizate (în acest caz, adresa poștală).

- o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a dispus o sancțiune cu amendă în cuantum de 3.200 de euro pentru insuficiența temeiului legal pentru prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost aplicată Primăriei din Kecskemét pentru dezvăluirea ilegală a informațiilor personale ale unui denunțător. NAIH a aplicat amenda după ce un angajat al unei organizații a depus o reclamație de interes public direct împotriva angajatorului său. După ce organizația a aflat despre plângere, a solicitat

detalii pentru a investiga, iar administrația locală a dezvăluit în mod accidental numele reclamantului.



DE REȚINUT! Autoritatea de supraveghere a considerat un factor agravant faptul că, în urma încălcării datelor, organizația a concediat persoana care a făcut raportul.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a sancționat un recuperator cu amendă în cuantum de 1.560 de euro pentru nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: O persoană vizată a solicitat informații și ștergerea datelor prelucrate, iar recuperatorul a refuzat. În scopul identificării, el a solicitat locul nașterii, numele fetei mamei și alte detalii de la persoana vizată. După ce operatorul a reușit să identifice persoanele vizate, el a refuzat să respecte cererea de ștergere, argumentând că este obligat legal să păstreze copii de rezervă.



DE REȚINUT! Invocarea unei obligații legale ar putea fi excesivă dacă în realitate, stocarea ulterior ștergerii are la bază interesele legitime ale operatorului.

o Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informațiilor (NAIH) a primit o sancțiune în cuantum de 1.560 de euro, motivul fiind nerespectarea principiilor generale de prelucrare.

Situația de fapt ce a stat la baza aplicării sancțiunii: O bancă a trimis în mod eronat mesaje despre datoria unui card de credit al unei persoane la numărul unei alte persoane. După ce a primit un număr de telefon incorect de la client în momentul contractării, banca nu a respectat solicitarea persoanei vizate de a șterge datele și a continuat să trimită un mesaj la numărul de telefon incorect.



DE REȚINUT! Operatorul trebuie să preîntâmpine astfel de incidente.

În anul 2018, NAIH a aplicat o singură sancțiune cu amendă în valoare de 3.200 de euro, motivul fiind neîndeplinirea suficientă a drepturilor persoanelor vizate.

Situația de fapt ce a stat la baza aplicării sancțiunii: Amenda a fost impusă pentru că nu s-au pus la dispoziția persoanei vizate înregistrările

de pe mijloacele de supraveghere video, pentru că nu s-au păstrat înregistrările pentru o utilizare ulterioară de către acea persoană și pentru că aceasta nu a fost informată despre dreptul său de a depune o plângere la autoritatea de supraveghere.



DE REȚINUT! Neinformarea persoanelor vizate cu privire la drepturile de care dispune conform prevederilor legale poate fi sancționată de către autoritatea de supraveghere.

Impactul Brexit asupra aplicării GDPR

Un aspect important de pus în discuție este legat de procesul de retragere a Regatului Unit din Uniunea Europeană (Brexit) ce a fost finalizat la 31 ianuarie 2020.

După cum deja știm, retragerea va opera, conform acordului de retragere, etapizat, până la finalizarea perioadei de tranziție, respectiv finalul anului 2020.

În Marea Britanie sunt aplicate GDPR și UK Data Protection Act 2018 în prezent și vor continua să fie aplicate până la sfârșitul perioadei de tranziție, astfel încât până în 2021 nu vor exista modificări în ceea ce privește prelucrarea datelor cu caracter personal. Din 2021, odată cu încheierea perioadei de tranziție, în Marea Britanie va fi aplicat un nou regim pentru prelucrarea datelor cu caracter personal, cunoscut drept „UK GDPR”. Totuși, nu există diferențe materiale majore față de GDPR, astfel încât operatorii de date personale vor aplica aceleași dispoziții ca în prezent.

Deși în cadrul prezentei lucrări nu ne-am mai oprit spre a analiza sancțiunile aplicate de ICO (Information Commissioner's Office) UK – autoritatea de supraveghere din Marea Britanie, considerăm în continuare faptul că practica acestei autorități și instrumentele puse la dispoziția operatorilor sunt de un real ajutor în elaborarea planurilor de conformare. O schimbare dată de Brexit va fi reprezentată și de faptul că ICO va fi autoritatea responsabilă de aplicarea UK GDPR.

O atenție deosebită va trebui acordată transferurilor internaționale de date personale, deoarece Marea Britanie va deveni țară terță. Conform GDPR, transferul de date personale din SEE către țări terțe este permis doar în anumite circumstanțe: dacă Comisia Europeană a emis o decizie de adecvare și dacă există garanții potrivite și suficiente.

Este important de menționat faptul că se dorește de către ambele părți (UE și Marea Britanie) obținerea unei decizii de adecvare până la sfârșitul perioadei de tranziție). UK GDPR a recunoscut automat ca adecvate toate statele membre UE.

Orice website sau companie din lume care prelucrează datele personale ale persoanelor fizice din Regatul Unit va respecta noile cerințe UK-GDPR. Astfel, companiile din UE care oferă servicii în Marea Britanie trebuie să desemneze un reprezentant. Acesta poate fi o persoană fizică sau juridică stabilită în Regatul Unit care reprezintă operatorul.

Procedura investigațiilor

În mod evident, având în vedere numărul mare al operatorilor, odată cu aplicarea GDPR, era previzibilă necesitatea impunerii unei noi proceduri prin intermediul căreia să fi trasate anumite direcții în conformitate cu care să se desfășoare investigațiile întreprinse de ANSPDCP. Reglementarea acestor aspecte era necesară atât din perspectiva asigurării unui echilibru în cazul unui control în ceea ce privește operatorii, precum și pentru stabilirea în mod clar a prerogativelor de care se bucură reprezentanții ANSPDCP.

Vom realiza, în cele ce urmează, o analiză a principalelor aspecte stabilite prin Decizia nr. 161/2018, dar și comentarii relevante de ajutor pentru operatorii care se confruntă cu o investigație sau care vor să cunoască elementele unui astfel de demers.

Modalitatea prin intermediul căreia este inițiată o investigație

Investigațiile întreprinse de ANSPDCP pot fi inițiate din oficiu sau în urma înregistrării unei plângeri. După cum poate fi observat, nu este obligatoriu ca inițierea investigației să fie urmarea unei plângeri adresate ANSPDCP astfel încât procedura investigației în ceea ce-i privește pe operatori poate fi demarată inclusiv ca urmare a unei rezoluții luate din oficiu de către Autoritate – în acest caz, este vorba practic despre o autosesizare.

Câteva astfel de exemple privind modalitățile în care pot începe investigațiile:

a) la propunerea compartimentelor cu atribuții de control ale ANSPDCP;

b) la propunerea președintelui sau vicepreședintelui ANSPDCP, printr-o rezoluție scrisă;

c) la propunerea celorlalte compartimente din cadrul ANSPDCP;

d) ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal;

e) pentru verificarea unor date și informații cu privire la prelucrarea datelor cu caracter personal, obținute de către ANSPDCP din alte surse decât cele care fac obiectul unor plângeri, inclusiv pe baza sesizărilor sau a informațiilor primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;

f) în vederea cooperării internaționale, precum și cu celelalte autorități de supraveghere din statele membre, în domeniul protecției datelor cu caracter personal, inclusiv în cadrul operațiunilor comune și al acordării de asistență reciprocă.

Dacă în ceea ce privește exemplele de la literele a)-c) și f), acestea privesc exclusiv autosesizarea ANSPDCP și demararea investigației ca urmare a unei note motivate care cuprinde entitatea supusă investigației, avizată de șeful ierarhic și aprobată de președintele ANSPDCP, în cazul literelor d) și e), putem observa că inițierea procedurii investigației are loc tot ca urmare a unei sesizări, însă ușor diferită.



Exemplu:

I) În ceea ce privește litera d), putem avea în vedere situația în care, în urma unei plângeri adresate ANSPDCP, se consideră că aceasta este neîntemeiată și nu se impune declanșarea procedurii investigației, dar, la momentul la care este analizată plângerea, Autoritatea observă o altă/alte nereguli în ceea ce privește prelucrarea datelor cu caracter personal. În acest caz, deși procedura nu este începută ca urmare a plângerii adresate ANSPDCP, are loc o autosesizare a instituției, astfel fiind declanșată procedura sesizării din oficiu.

II) Cu referire la litera e), este avută în vedere situația în care prin intermediul diferitelor canale precum: „corespondența primită de ANSPDCP, mass-media, accesarea rețelei de internet, documentele de constatare întocmite în urma efectuării altor investigații sau alte documente de la nivelul ANSPDCP, activitățile de cooperare cu entități de drept public sau privat ori cu autorități de supraveghere din străinătate”, sunt primite informații referitoare la acțiuni ce vizează un anumit operator care efectuează acțiuni de prelucrare cu încălcarea dispozițiilor GDPR.

După cum am menționat mai sus, în cadrul celor două cazuri de inițiere a procedurii investigației din oficiu, sunt avute în vedere situații în care, inițial, Autoritatea este totuși „sesizată”, deși impropriu, prin diferite modalități: mediul online, plângere neîntemeiată care vizează un anumit fapt, mass-media etc. În mod evident, cazurile enumerate mai sus în cadrul exemplului II) nu sunt nicidecum exhaustive, situațiile ce pot apărea putând fi extrem de numeroase.



ATENȚIE! Totuși, atragem atenția că, în ceea ce privește eventualele atribuții ale personalului din cadrul departamentului IT/marketing al societăților, acesta ar trebui să supravegheze cu foarte mare atenție conținutul eventualelor publicații ce fac publice postări referitoare la modalitatea de prelucrare a datelor de către respectiva entitate. Totodată, atenția trebuie să fie sporită și pentru materialele publicate sau aprobate de societatea însăși, care, desigur, pot cuprinde informații „de interes” pentru Autoritate.

Așadar, concluzionând, simplul fapt al inexistenței unei sesizări din partea persoanelor interesate nu conduce în mod obligatoriu la ideea că în cazul operatorului de date cu caracter personal nu poate fi inițiată procedura desfășurării unei investigații.

Controlul efectuat de ANSPDCP este întotdeauna anunțat?

Conform procedurii investigației, controlul efectuat de către Autoritate poate fi inițiat atât cu înștiințarea prealabilă a operatorului verificat, dar și inopinat, fără anunțarea în prealabil a entității controlate.

Dacă în ceea ce privește controlul inopinat, entitatea controlată nu este anunțată și Autoritatea nu are nicio obligație în ceea ce privește furnizarea de detalii referitoare la investigație, atunci când avem în vedere controlul efectuat prin anunțarea prealabilă a entității verificate, notificarea trebuie să conțină atât data cât și intervalul orar în care va avea loc inspecția.

Metoda controlului efectuat prin anunțarea prealabilă a operatorului este utilizată cu precădere atunci când ANSPDCP dorește să se asigure că nu vor exista documente ce țin de protecția datelor cu caracter personal pe care operatorul nu ar putea să le pună la dispoziție. În acest sens, precizăm că printre activitățile pe care le poate desfășura personalul ANSPDCP se număra și „verificarea oricărui document, echipament,

mijloc sau suport de stocare a datelor necesare desfășurării investigației;” sau „ridicarea documentelor, în copie certificată de către entitatea controlată sau a înregistrărilor relevante care au legătura cu obiectul controlului și anexarea acestora la procesul-verbal de constatare/sanționare”. În același timp, entitatea controlată are obligații precum: „să pună la dispoziția personalului de control orice informații și documente indiferent de suportul de stocare, necesare desfășurării investigației, inclusiv copii de pe acestea”, „să pună la dispoziția ANSPDCP documentele solicitate, certificate pentru conformitate cu originalul”, „să furnizeze într-o formă completă documentele, informațiile, înregistrările și evidențele solicitate, precum și orice lămuriri necesare, fără a putea opune caracterul confidențial al acestora, în condițiile legii”.

Pot amâna efectuarea unei investigații anunțate?

S-ar presupune, la o primă vedere, că nu există niciun motiv pentru care s-ar putea dispune amânarea unei investigații, atât timp cât a existat o notificare transmisă în prealabil în mod corespunzător și dat fiind faptul că o autoritate a statului solicită în mod ferm detalii referitoare la desfășurarea activității unui operator de date cu caracter personal. Totuși, art. 15 din procedura de efectuare a investigațiilor permite ANSPDCP amânarea sau chiar, în anumite cazuri, suspendarea procedurii investigației pentru motive justificate. Desigur, de cele mai multe ori, operatorii controlați vor solicita aplicarea art. 15 privind suspendarea sau amânarea efectuării investigațiilor și tot acestora, în mod evident, le va reveni și sarcina dovedirii unor motive justificate pentru care investigația nu ar putea avea loc la data stabilită.

Noțiunea de motive justificate este una extrem de vagă ce poate suporta diferite interpretări, motiv pentru care putem doar să ne stabilim cu titlu general câteva ipoteze în cazul cărora ar putea să fie incidentă aplicabilitatea art. 15 din procedura de efectuare a investigațiilor:

1) Lipsa responsabilului cu protecția datelor desemnat în prealabil de operator – evident în cazurile în care desemnarea unui asemenea responsabil este necesară conform GDPR. Fiind persoana desemnată pentru gestionarea activităților de prelucrare a datelor cu caracter personal, lipsa acesteia ar putea conduce la imposibilitatea efectuării unui control în mod corespunzător. Pentru clarificare, amintim că desemnarea unui responsabil cu protecția datelor se impune în situația în care avem în vedere o prelucrare pe scară largă a unor categorii speciale de date cu

caracter personal cum ar fi cele referitoare la originea rasială sau etnică, date biometrice, date privind sănătatea precum și, în egală măsură, atunci când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;

2) Informațiile solicitate de către ANSPDCP vizează furnizarea unui număr de documente care nu pot fi aduse în timp util. Putem lua drept exemplu situația în care documentele necesare investigației au fost arhivate, iar acestea sunt păstrate de către o societate specializată care se ocupă cu arhivarea documentelor. În situația în care data la care se va desfășura investigația anunțată de către autoritate nu permite aducerea unor astfel de documente, acest temei ar putea reprezenta un motiv justificat pentru care investigația nu poate avea loc în condiții corespunzătoare. Desigur, trebuie avută în vedere și importanța documentelor în cadrul investigației și aportul pe care îl pot aduce acestea în ceea ce privește rezoluția adoptată de către ANSPDCP.

3) În lipsa unuia din responsabilii privind protecția datelor cu caracter personal – este posibil ca informațiile necesare investigației să poată fi furnizate de către persoane din cadrul mai multor departamente ale operatorului (marketing, financiar etc.). Dacă aceste persoane nu pot fi prezente simultan astfel încât fiecare departament să poată prezenta în mod corespunzător documentele ce privesc prelucrarea datelor cu caracter personal, operatorul ar putea folosi acest motiv și solicita o amânare a investigației.

Desigur, exemplele de mai sus pot continua în funcție de situațiile practice concrete ce pot apărea, iar fiecare caz în mod evident va avea particularitățile sale urmând ca modalitățile în care poate fi suspendată/amânată o investigație să fie analizate în particular.

Desfășurarea efectivă a procedurii investigației

În legătură cu procedura concretă de desfășurare a unei investigații întreprinse de către ANSPDCP, sunt anumite precizări de făcut atât în ceea ce privește modalitățile în care se poate desfășura investigația, parcursul efectiv al investigației cât și drepturile și obligațiile atât în ceea ce privește autoritatea ce efectuează investigația cât și operatorul de date supus investigației.

Mai întâi, în ceea ce privește locul în care pot avea loc investigațiile conduse de ANSPDCP, art. 16 din procedura ce reglementează desfășurarea investigațiilor stabilește că acestea pot avea loc pe teren, la sediul autorității ori în scris.

Efectuarea investigațiilor pe teren

Investigațiile pe teren sunt caracterizate de verificările efectuate la sediul/domiciliul/ punctul de lucru sau alte locații unde își desfășoară activitatea operatorul sau locații care au legătură cu prelucrarea în cauză, după caz. Cu alte cuvinte, acest tip al investigației este caracterizat de prezența fizică a autorității la locul unde își desfășoară activitatea operatorul verificat.

În cadrul acestei proceduri, personalul autorizat ANSPDCP desfășoară în ordine următoarele activități descrise în cadrul procedurii ce detaliază efectuarea investigațiilor: deplasarea la sediul la sediul/domiciliul/punctul de lucru sau alte locații sau, de ce nu, alte locații la care își desfășoară activitatea operatorul verificat, prezentarea documentelor ce țin de legitimarea reprezentanților care urmează să efectueze operațiunile de verificare, înscrierea în registrul de control al entității controlate a datelor aferente persoanelor ce efectuează controlul (numele și prenumele persoanelor împuternicite de a efectua controlul, unitatea de care aparțin, numărul legitimației de control, numărul și data delegației/ordinului de deplasare, obiectivele controlului, perioada controlului, perioada controlată, precum și temeiul legal în baza căruia se efectuează controlul), prezentarea obiectivelor investigației, verificarea tuturor aspectelor ce țin de investigație (atat documente cât și mijloace tehnice), ridicarea documentelor în copie certificată de către operator și, nu în ultimul rând, întocmirea procesului-verbal de constatare/sanționare, prin evidențierea situațiilor prezentate de entitatea controlată, a declarațiilor reprezentanților acesteia și a constatărilor proprii și aplicarea de sancțiuni contravenționale sau a altor tipuri de măsuri corective, după caz. Important de menționat este faptul că trebuie înmănată și o copie a procesului-verbal întocmit către entitatea controlată.

Un aspect particular al investigațiilor desfășurate pe teren este acela al împiedicării în orice fel a efectuării controlului de către entitatea verificată. Pentru astfel de evenimente, există o procedură special descrisă de art. 20 din decizia ce reglementează investigațiile. Astfel, în situația în care autoritatea este împiedicată în orice mod în exercitarea atribuțiilor, poate

solicita o autorizare judiciară, a cărei caracteristica principală este reprezentată de celeritatea cu care este emisă, fiind vorba despre o încheiere pronunțată de către președintele Curții de Apel București sau, în lipsa sa, un judecător delegat de acesta. Cu alte cuvinte, autorizarea acordată de către instanță poate fi asemănată unui „mandat” specific dreptului penal prin intermediul căruia este permis accesul forțat al autorităților.



Atenție! O copie a autorizației emise de către Curtea de Apel București trebuie comunicată și către entitatea controlată înainte de începerea investigației. Acest aspect este unul extrem de important dat fiind faptul că, în primul rând, lipsa unei comunicări a încheierii nu ar putea echivala cu o procedură completă, iar în al doilea rând, încheierea pronunțată poate fi atacată cu contestație la Înalta Curte de Casație și Justiție în termen de 72 de ore de la comunicarea acesteia, însă formularea căii de atac nu suspendă executarea. Practic, după ce a fost comunicată încheierea către operatorul investigat, formularea unei căi de atac nu conduce la întreruperea efectuării investigației.

Cu privire la intervalul orar în care poate avea loc investigația, în toate situațiile procedura investigației nu poate începe înainte de ora 08:00 și nu poate continua după ora 18:00. Desigur, dispozițiile legale prevăd și posibilitatea ca investigația poate continua și după ora 18:00 numai cu acordul persoanei la care se efectuează aceasta sau a reprezentantului său. Nu în ultimul rând, actele de verificare trebuie efectuate în prezența persoanei la care se efectuează investigația sau a reprezentantului său.

Dacă am transpune aceste dispoziții într-o situație practică, ar însemna că operatorul ar trebui să aibă o persoană desemnată care să fie alături de reprezentanții ANSPDCP pe tot parcursul efectuării investigațiilor, astfel încât să se asigure că nu există abuzuri.

O prerogativă extrem de importantă și interesantă recunoscută inspectorilor ANSPDCP este aceea a audierii persoanelor ale căror declarații sunt considerate relevante și necesare desfășurării investigației. Un aspect important ar fi că procedura prevede doar posibilitatea refuzului de a semna rezultatul audierii (cu menționarea refuzului în mod corespunzător), nu și posibilitatea de a refuza audierea în mod efectiv. Acest lucru s-ar putea traduce practic în obligativitatea participării persoanelor la audiere dar cu posibilitatea de a refuza furnizarea de informații sau de a răspunde prin „nu cunosc”.

Efectuarea investigațiilor la sediul ANSPDCP

Și în acest caz, capitolul în cadrul căruia este descrisă procedura este extrem de sugestiv în ceea ce privește locul și modul în care are loc investigația efectuată de către A.N.S.P.D.C.P. Investigația în acest caz începe prin trimiterea unei „*invitații*” denumită legal în cadrul deciziei care reglementează procedura „adresa de convocare”, în cuprinsul căreia este menționată data și ora începerii investigației la sediul A.N.S.P.D.C.P.

Adresa de convocare conține toate detaliile necesare entității convocate la investigație, cum ar fi documentele necesare, înregistrări relevante, echipamente informatice în funcție de obiectul controlului, actele de identitate ale reprezentantului legal/persoanei împuternicite și ale entității controlate și alte asemenea. Putem spune că acest tip de investigație este mai puțin intruziv în ceea ce privește „*intimitatea*” Operatorului dat fiind faptul că reprezentanții A.N.S.P.D.C.P. nu se mai deplasează la sediul Operatorului/locul unde are loc prelucrarea datelor cu caracter personal.

Totuși, interesant de precizat în ceea ce privește acest tip de procedura este că Autoritatea ar putea încheia procesul-verbal conform detaliilor ce au fost precizate mai sus, inclusiv fără convocarea reprezentanților Operatorului investigat, în situația în care se conchide că există dovezi suficiente/relevante pentru finalizarea investigației, aspect precizat în mod expres în cadrul art. 32 din Decizia ce reglementează desfășurarea procedurii. Prin urmare, în acest caz în care investigația are loc la sediul A.N.S.P.D.C.P., autoritatea ar putea dispune sancționarea Operatorului investigat atunci când, în urma analizării situației pentru care a fost dispusă începerea investigației împreună cu probatoriul rezultat, constata că există un material suficient care ar putea conduce la ideea conform căreia Operatorul ar putea fi sancționat/avertizat pentru prelucrarea necorespunzătoare.

Efectuarea investigațiilor în scris

Desfășurarea procedurii investigației în scris presupune lipsa oricărui contact direct între Operatorul investigat și A.N.S.P.D.C.P. Este, după cum rezultă din descrierea capitolului în cadrul căruia sunt descrise modalitățile de efectuare a acestui tip de investigație, una dintre cele mai simple modalități de verificare a unui Operator, comunicările dintre reprezentanții Operatorului și Autoritate desfășurându-se prin intermediul transmiterii

folosind mijloace de comunicare la distanță a tuturor documentelor necesare desfășurării investigației.

Concret, entitatea investigată va primi din partea reprezentanților A.N.S.P.D.C.P. o adresă prin intermediul căreia îi vor fi solicitate informațiile și documente pe care titularul lucrării le găsește necesare pentru a soluționa investigația începută. Nu există o enumerare exhaustivă a informațiilor sau documentelor ce pot fi solicitate Operatorului, astfel încât ne putem aștepta la solicitări ce vizează diferite politici interne, proceduri, registre etc. Desigur, toate acestea vor avea relevanță în ceea ce privește investigația întreprinsă.

După ce răspunsul operatorului este primit de către reprezentanții Autorității, procedura desfășurării investigației recunoaște acestora următoarele posibilități: i) continuarea investigației în scris; ii) continuarea investigației însă transformarea acesteia într-o investigație pe teren; iii) finalizarea investigației prin încheierea procesului-verbal în mod corespunzător.

Astfel cum poate fi liber observat, chiar dacă Operatorul se conformează tuturor solicitărilor indicate în cadrul adresei primite din partea reprezentanților A.N.S.P.D.C.P., este posibil ca autoritatea să considere că investigația trebuie să continue și, astfel, să fie solicitate inclusiv alte documente pe care Autoritatea le va considera necesare. Acest fapt ar putea fi tratat asemenea unei consecințe naturale a analizării documentelor înaintate Autorității, analiză în urma căreia persoana desemnata nu poate dispune încheierea investigației dat fiind faptul probele pot fi insuficiente sau, de ce nu, din cadrul probelor analizate să rezulte alte modalități de prelucrare neconforme.

În egală măsură, tot în urma examinării documentelor transmise de Operator, Autoritatea ar putea considera necesară conversiunea procedurii investigației desfășurate în scris, în procedura investigației efectuate pe teren, cu respectarea dispozițiilor prezentate mai sus, în cadrul secțiunii aferente. Schimbarea procedurii investigației ar putea opera, spre exemplu, atunci când, urmare a analizării documentelor solicitate și depuse de Operator, rezultă operațiuni de prelucrare a datelor cu caracter personal care, din punct de vedere al legislației aplicabile nu sunt tocmai conforme și astfel trebuie analizate în mod particular, fiind necesară inclusiv deplasarea la sediul Operatorului de date.

Ulterior analizării documentelor, personalul de control poate să sancționeze/avertizeze Operatorul în cauză prin intermediul unui proces-verbal despre care vom discuta mai jos, caracteristicile acestuia fiind aceleași pentru oricare dintre procedurile de investigație. Totuși, în

situația în care personalul de control apreciază că nu este necesară măsura întocmirii unui proces-verbal în urma investigației, acesta poate apela la realizarea unei note de finalizare a investigației prin intermediul căreia să constate că în urma administrării și analizării tuturor probelor investigația se poate finaliza fără a întreprinde alte demersuri suplimentare.



Atenție! Dată fiind posibilitatea de a finaliza investigația prin intermediul unei astfel de note de finalizare, pentru a fi valabilă, bineînțeles aceasta trebuie confirmată și avizată de șeful ierarhic și aprobată de președintele A.N.S.P.D.C.P. Acesta din urmă poate și delega această atribuție șefului compartimentului de control care a efectuat investigația.

Aspecte particulare privind investigațiile desfășurate la autoritățile/organismele publice

În cazul controlului efectuat ce vizează autoritățile sau organismele publice, procedura desfășurării investigației presupune anumite derogări specifice pe care le vom prezenta în cele ce urmează.

Ulterior finalizării unei investigații efectuate în cadrul unei autorități publice, echipa de control desemnată din cadrul A.N.S.P.D.C.P. poate încheia un proces-verbal de constatare/sanționare prin care se aplică sancțiunea avertismentului și la care anexează un plan de remediere. Planul de remediere este un instrument folosit exclusiv în cadrul acestui tip de investigație și presupune indicarea faptelor care constituie acțiuni contrare GDPR, măsurile pentru remediere propuse de personalul specializat, termenul în care acestea trebuie aduse la îndeplinire și modalitatea de implementare a măsurilor. Formatul acestui plan este standardizat și este inclus în anexa legii nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679:

Plan de remediere ziua luna anul – Modul de îndeplinire a măsurilor de remediere

Nr.	Fapta săvârșită	Măsuri de remediere	Termen de remediere	Mod de îndeplinire

Nr.	Fapta săvârșită	Măsuri de remediere	Termen de remediere	Mod de îndeplinire

Alte mențiuni

.....

.....

Agent constator/
Persoana competentă,

.....
(numele, prenumele, semnătura)

Contravenient

.....
(numele, prenumele, semnătura)

Stampila

În funcție de complexitatea măsurilor ce trebuie implementate, referenții ANSPDCP stabilesc un termen pentru planul de remediere impus autorității publice. Dacă ar fi să analizăm dispozițiile legale privind efectuarea investigațiilor, până la expirarea acestui termen, ANSPDCP nu poate aplica nicio sancțiune organismului public. Raportat la termenul acordat pentru remediere, ulterior, în termen de 10 zile, Autoritatea va putea relua controlul în ceea ce privește această categorie specială a Operatorilor de date cu caracter personal. Dacă, în urma acestui control subsecvent, Autoritatea va constata că măsurile stabilite în sarcina autorității publice nu au fost puse în executare, va putea aplica sancțiunea contravențională a amenzii.

Procesul-verbal încheiat de ANSPDCP. Elemente componente. Căi de atac. Posibile sancțiuni

După cum menționam în rândurile precedente, finalizarea procedurii se definitivează prin încheierea procesului-verbal (cu excepția cazului în care avem în vedere redactarea unei note de finalizare – posibilă în cazul investigației în scris – sau stabilirea unui plan de remediere), urmând ca o copie a acestuia să fie înmânata reprezentantului Operatorului, acesta din urmă având posibilitatea contestării procesului-verbal în termen de 15 zile de la data comunicării (atunci când procesul-verbal a fost încheiat în lipsa lui și i-a fost comunicat ulterior), respectiv de la data înmânării (atunci când reprezentanții Operatorului au fost prezenți la încheierea procesului-verbal).

Cu alte cuvinte, din punct de vedere practic, toate activitățile, inclusiv rezultatul investigației sunt menționate în procesul-verbal de constatare/sancționare încheiat de personalul de control. Există o serie de elemente pe care procesul-verbal trebuie să le conțină în mod obligatoriu, sub sancțiunea nulității absolute a procesului-verbal, lipsa oricăreia dintre următoarele mențiuni putând fi contestată în fața instanței competente și putând conduce la anularea procesului-verbal de constatare/sancționare:

a) data și locul încheierii procesului-verbal de constatare/sancționare;
b) datele de identificare și funcțiile membrilor echipei de control, inclusiv numărul legitimației de control;

c) numărul și data deciziei de împuternicire emise de președintele ANSPDCP și, după caz, numărul și data împuternicirii pentru investigațiile efectuate pe teren și neanunțate în prealabil în scris;

d) obiectul controlului;

e) datele de identificare ale entității controlate;

f) datele de identificare și funcțiile reprezentanților entității controlate;

g) constatările rezultate în urma verificărilor efectuate;

h) descrierea faptei contravenționale, cu indicarea datei și locului în care a fost săvârșită fapta, a împrejurărilor ce pot servi la aprecierea gravității faptei și, eventual, a pagubelor, a actului normativ prin care se stabilește și se sancționează contravenția, precum și a măsurilor corective și/sau a sancțiunii aplicate, dacă este cazul;

i) termenul de exercitare a căii de atac și instanța la care se depune plângerea, în cazul aplicării unei sancțiuni contravenționale;

j) dacă s-au ridicat documente sau alte materiale, felul și natura acestora;

k) dacă reprezentanții entității controlate, care au participat la activitatea de control, au refuzat să consemneze obiecțiunile cu privire la conținutul procesului-verbal de constatare/sancționare, după ce le-a fost adus la cunoștința acest drept;

l) mențiuni privind înmânarea/comunicarea procesului-verbal de constatare/sancționare, în copie, reprezentanților entității controlate;

m) motivele pentru care reprezentanții entității controlate nu au semnat procesul-verbal de constatare/sancționare, cu indicarea datelor de identificare a martorului care atesta motivele nesemnării procesului-verbal, în cazul în care acesta exista, sau a motivelor care au condus la întocmirea procesului-verbal în lipsa unui martor. Alte aspecte importante cu privire la redactarea procesului-verbal sunt reprezentate de faptul că o copie a acestuia trebuie înmănată persoanei la care a avut loc controlul, iar acesta trebuie semnat pe fiecare pagină de către membrii echipei de control și de

către reprezentanții legali sau desemnați ai entității controlate. Totodată, procesul-verbal reprezintă și titlu de creanță și înștiințare de plată, conform dispozițiilor legale. Acest lucru înseamnă că prin primirea procesului-verbal persoana a luat cunoștința de conținut, însă, până la împlinirea termenului nu poate obliga la achitarea obligațiilor fiscale (care trebuie plătite benevol), însă, după expirarea termenului de plată, acesta se transforma în titlu executoriu prin efectul legii, moment de la care entitatea obligată la plată poate fi obligată să execute silit datoriile fiscale.

Sanțiunile principale ce pot fi aplicate de către A.N.S.P.D.C.P. sunt avertismentul și amenda. În situația în care amenda este mai mică de 300.000 de euro, aceasta se poate aplica direct prin intermediul procesului-verbal încheiat de reprezentanții A.N.S.P.D.C.P. În cazul în care amenda este mai mare de 300.000 de euro, aplicarea sancțiunii se va face prin decizie a președintelui A.N.S.P.D.C.P., care are la bază procesul-verbal de constatare și raportul personalului de control. De asemenea, A.N.S.P.D.C.P. poate dispune, prin decizie a președintelui care constituie, de altfel, titlu executoriu, aplicarea unei amenzi cominatorii de până la 3.000 de lei pentru fiecare zi de întârziere, calculată de la data stabilită prin decizie, în situația în care nu sunt respectate măsurile corective aplicate de Autoritate sau în cazul refuzului tacit sau expres de furnizare a tuturor informațiilor și documentelor solicitate în cadrul procedurii de investigație ori în cazul refuzului de supunere la investigație, potrivit legii.

Sanțiunile principale pot fi aplicate alături de anumite măsuri corective cum ar fi: obligarea Operatorului sau a persoanei împuternicite de Operator să respecte cererile persoanei vizate de exercitare a drepturilor, să asigure conformitatea operațiunilor de prelucrare cu dispozițiile legale aplicabile, obligarea Operatorului să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal, limitarea temporară sau definitivă, interdicția asupra prelucrării, rectificarea sau ștergerea datelor cu caracter personal, restricționarea prelucrării, notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, retragerea unei certificări sau obligarea organismului de certificare să retragă o certificare eliberată sau să nu elibereze o certificare în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite, precum și suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională. Asemenea procesului-verbal despre care am menționat mai sus, decizia prin intermediul căreia să impună anumite măsuri corective trebuie să fie comunicată entităților controlate și trebuie să conțină în mod obligatoriu:

datele de identificare ale ANSPDCP și numele reprezentantului legal al acesteia, datele de identificare ale operatorului/persoanei împuternicite de operator descrierea faptelor și a împrejurărilor care pot fi avute în vedere la individualizarea măsurii, indicarea temeiului legal potrivit căruia se stabilește și se sancționează fapta, măsurile corective aplicate, termenul și modalitatea de plată a amenzii, după caz, termenul de exercitare a căii de atac și instanța de judecată competentă.

B.C.U. „M.EMINESCU” IAȘI
ȘTIINȚE ECONOMICE

Librăria ta de carte de specialitate juridică, economică și business

Din 2008 suntem
alegerea lor...

TU?



Cursuri universitare • Tratatate • Monografii • Coduri • Legislație • Jurisprudență • Reviste de specialitate

www.ujmag.ro

ujmagro
UNIVERSUL JURIDIC MAGAZIN

Bd. Iuliu Maniu nr. 7, clădirea Cotroceni Business Center corp C,
sector 6, București (lângă AFI MALL)

021.312.22.21 | 0733.673.555 | comenzi@ujmag.ro

Universul Juridic

nihil sine iure



instrument
de pregătire
profesională

PARTENERIAT

Suntem o comunitate impresionantă
– peste 40.000 de membri activi

ONLINE

Conținut juridic de calitate disponibil
de pe orice dispozitiv:
laptop, mobil sau tabletă

REZULTATE

Puteți accesa informații juridice reale, certificate
editorial, necesare activității dvs., în orice moment,
sub semnătura specialiștilor recunoscuți în domeniu

TRADIȚIE

În 18 ani am devenit cel mai important actor al
pieței editoriale juridice! Peste 2.000 de titluri,
1.000 de autori, 12 reviste juridice. Acum și online!

ARTICOLE

Peste 10.000 de pagini de conținut
profesional structurat pe 12 secțiuni,
pentru a facilita accesul la conținutul relevant

LEGISLAȚIE

Modificări legislative, legi promulgate,
decizii CCR și ICCJ, proiecte de legi

ALĂTURĂ-TE CELOR 40.000 de profesioniști!
BENEFICIAZĂ de avantajele contului premium: GO PREMIUM!
Testează și convinge-te!

www.universuljuridic.ro

Cartea este o publicație de bune practici pe care orice om de afaceri ar trebui să o consulte de fiecare dată când ia decizii privind prelucrarea datelor cu caracter personal și nu numai.

Lucrarea este explicită, scrisă într-un limbaj clar și accesibil oricărei tipologii de cititor, dar mai ales este relevantă pentru că este scrisă de avocați cu multă experiență în domeniu, aducând noutăți prin exemplele aplicate pe care le oferă.

Astfel, consider că ar trebui să se regăsească în biblioteca de business a oricărui antreprenor.

CRISTINA TIMIȘ

Vicepreședinte CRIS-TIM



Elena GRECU



Raluca COMĂNESCU



Georgiana TRIFAN

Această carte a fost redactată cu obiectivul de a reprezenta un real sprijin pentru orice companie care dorește să se conformeze prevederilor legale și bunelor practici în materia protecției datelor cu caracter personal.

„GDPR pentru afaceri” conține informații accesibile, însoțite de exemple practice, care sunt analizate și explicate într-o manieră care să conducă la o implementare facilă. Este construită în mod gradual, pornind de la noțiunile teoretice, continuând cu explicarea acestora prin exemple concrete și încheind cu analiza și interpretarea unor cazuri punctuale de nerespectare a normelor privind protecția datelor cu caracter personal, desprinse din practica autorităților de supraveghere, evidențiată la nivel național și european.

Ghidul oferă recomandări cu privire la măsurile de adoptat în vederea asigurării unui nivel optim de conformare, astfel încât prelucrarea de date efectuată la fiecare nivel al companiilor să fie aliniată dispozițiilor în materie. Lucrarea poate fi urmată îndeaproape nu doar de departamentele-cheie ale unei companii, ci și de conducerea acesteia și de responsabilul cu protecția datelor personale desemnat.

Avantajul cărții este acela că oferă cititorilor săi un instrument practic care descifrează reglementările aplicabile și deschide drumul unei implementări responsabile a unui plan de conformare și nu a uneia pur formale.